UNIVERZITA PAVLA JOZEFA ŠAFÁRIKA V KOŠICIACH

Financované Európskou úniou NextGenerationEU

PLÁN OBNOVY

MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY

Bezpečnosť prevádzky a riešenie kybernetických incidentov

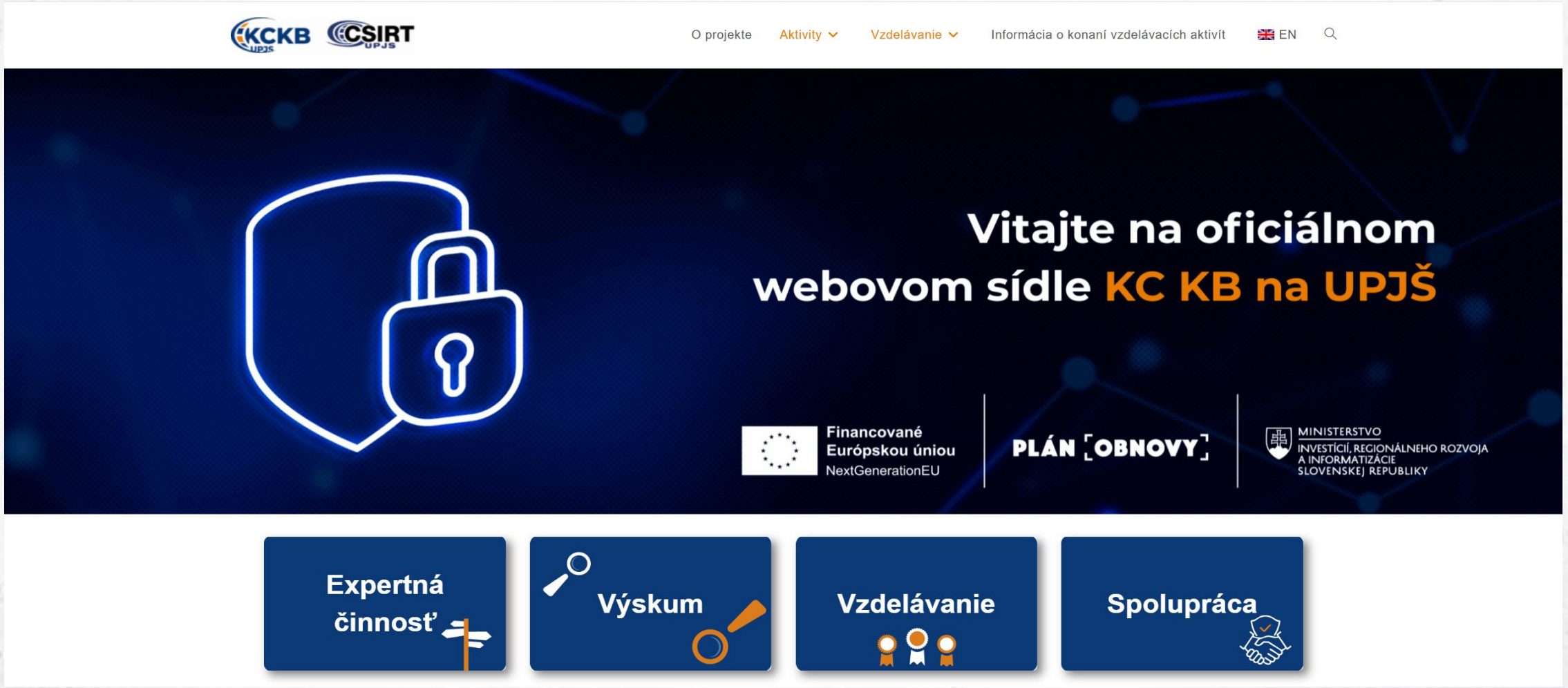
(Vzdelávanie pre zamestnancov verejnej správy v kategórii používateľov „laik“, „odborný zamestnanec“ a „manažér“ – modul č. 4)

Meno Priezvisko

XX.XX.XXX

KC KB UPJŠ

https://**cyberawareness.sk/**



Vzdelávacia aktivita (I.)

- Časový harmonogram
  - 08:30 – 10:00 – 1. blok
  - 10:00 – 10:15 – prestávka
  - 10:15 – 11:45 – 2. blok
  - 11:45 – 12:45 – prestávka
  - 12:30 – 14:00 – 3. blok
  - 14:00 – 15:30 – 4. blok

Vzdelávacia aktivita (II.)

Číslo modulu	Názov modulu	Časová dotácia (45 min.)	Forma stretnutia
Modul č. 1	Úvod do kybernetickej a informačnej bezpečnosti (KIB)	6	Online / Prezenčne
Modul č. 2	Kritické myslenie a dezinformácie	8	Online / Prezenčne
Modul č. 3	Sociálne inžinierstvo	8	Online / Prezenčne
Modul č. 4	Bezpečnosť prevádzky a riešenie kybernetických incidentov	8	Online / Prezenčne
Modul č. 5	Digitálna identita a súkromie v online prostredí	6	Online / Prezenčne
Modul č. 6	Základy práva informačných a komunikačných technológií pre KIB I.	8	Online / Prezenčne
Modul č. 7	Základy práva informačných a komunikačných technológií pre KIB II.	8	Online / Prezenčne

Škodlivý kód (I.)

Zdroj: ENISA Landscape 2024, https://www.enisa.europa.eu/publications/enisa-threat-landscape-2024

Ransomware froze more cities in 201
Next year is a toss-up

More than 70 state and local governments across the US suffered ransomware attacks in 2019.

Alfred Ng December 5. 2019 5:00 AM PST

Holandskú univerzitu ochromil na Vianoce kybernetický útok

Malware | Viry | Ransomware

Ransomware ve francouzské nemocnici zablokoval počítače. Personál se vrátil k tužce a papíru

Karel Kilián
26. listopadu 2019

SDÍLET NA FACEBOOKU TWEETNOUT

Zdroj: https://www.infosecurity-magazine.com/news/french-hospital-crippled-by/, https://www.cnet.com/culture/ransomware-devastated-cities-in-2019-officials-hope-to-stop-a-repeat-in-2020/, https://digitalportal.sk/holandsku-univerzitu-ochromil-na-vianoce-kyberneticky-utok/, https://www.zive.cz/clanky/ransomware-ve-francouzske-nemocnici-zablokoval-pocitace-personal-se-vratil-k-tuzce-a-papiru/sc-3-a-201359/default.aspx

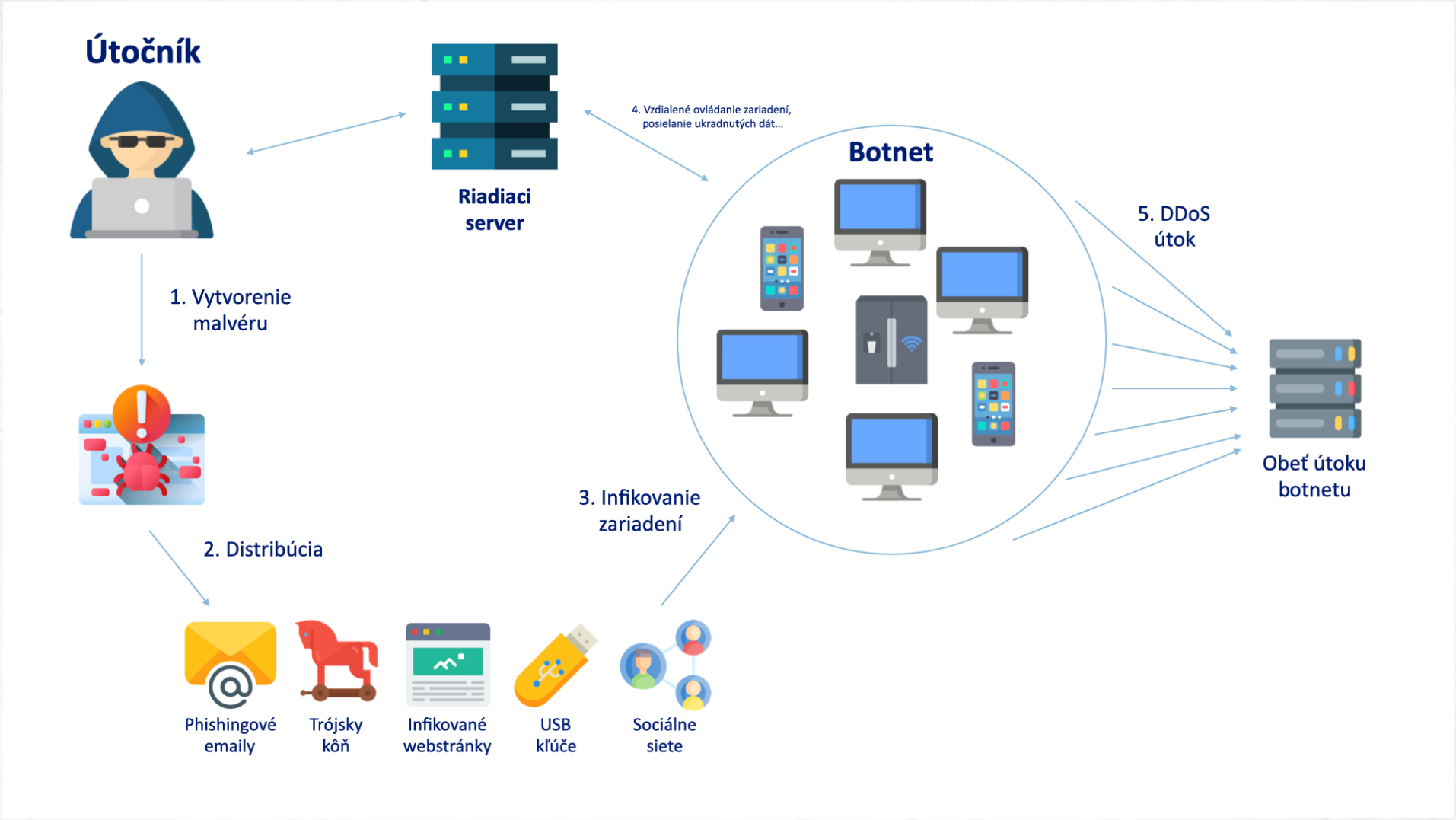
Zdroj: http://usa.kaspersky.com/internet-security-center/internet-safety/Malware-remover-vs-antivirus-software#.V2nAEriLSW8/

Malware = Malicious Software = Škodlivý kód

- Zadné vrátka – prístup do počítača odkiaľkoľvek
- Ťaženie kryptomien
- Súčasť botnetov
- Prístup k účtom
- Zasielanie údajov
- Stiahnutie ďalšieho škodlivého kódu
- Šifrovanie a výkupné

Zdroj: https://www.heise.de/news/Malware-saugte-Nutzerdaten-bei-1 671.html

Malvér



Zdroj: Martina Pivarníková, CSIRT.SK

Distribúcia malvéru (I.)

- Phishingové emaily
- Nebezpečné webové stránky

Zdroj: https://d32exi8v9av3ux.cloudfront.net/blog/Phishing2.2.png

Distribúcia malvéru (II.)

- Phishingové emaily
- Nebezpečené webové stránky
- Reklamy vo webových stránkach
- Upload/download dokumentov

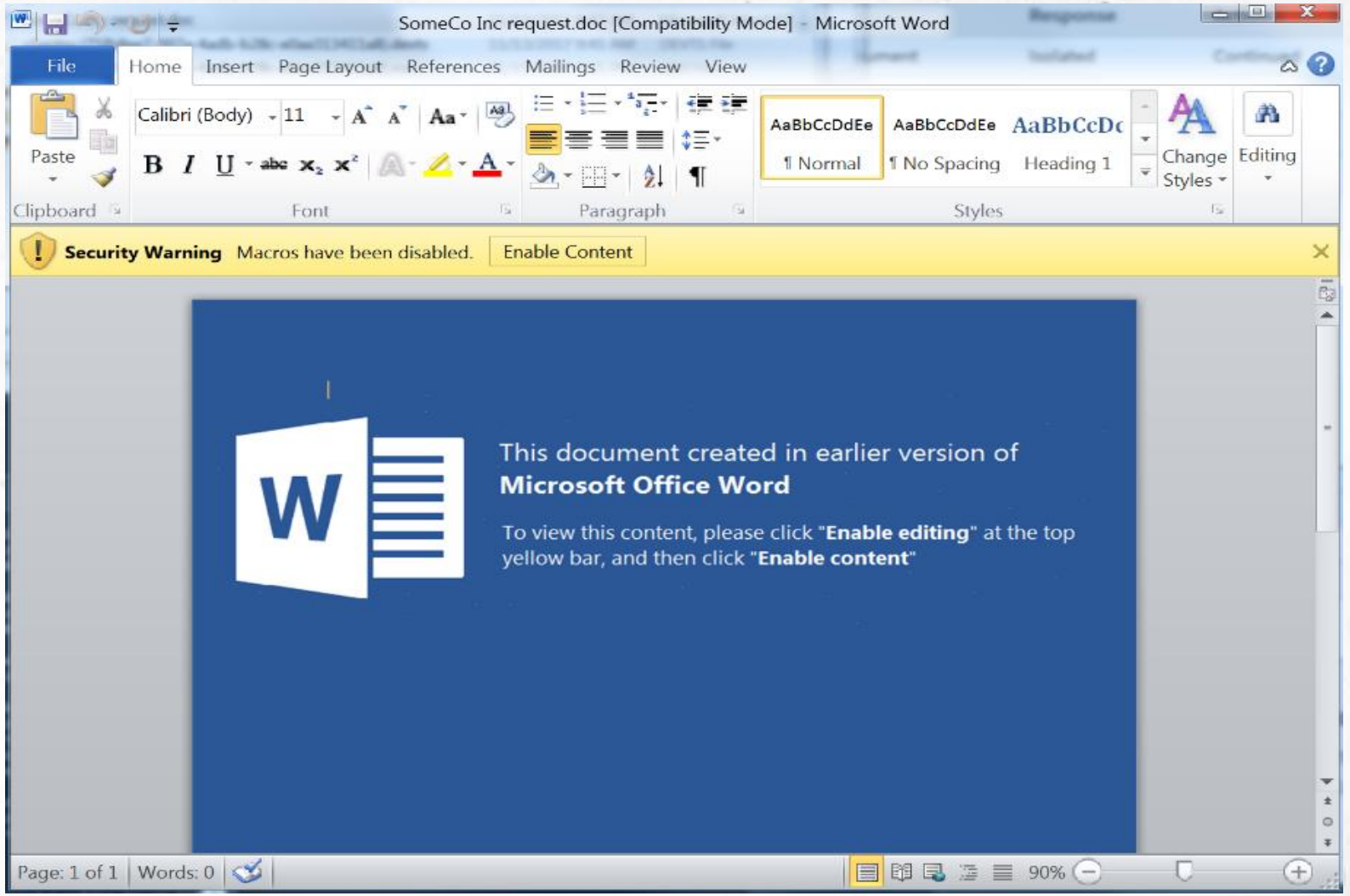
Zdroj: http://guides.uufix.com/wp-content/uploads/2017/06/adware.png

Distribúcia malvéru (III.)

- Phishingové emaily
- Nebezpečené webové stránky
- Reklamy vo webových stránkach
- Upload/download dokumentov
- Nezabezpečená sieť
- Fyzický prístup k počítaču (cez USB kľúče

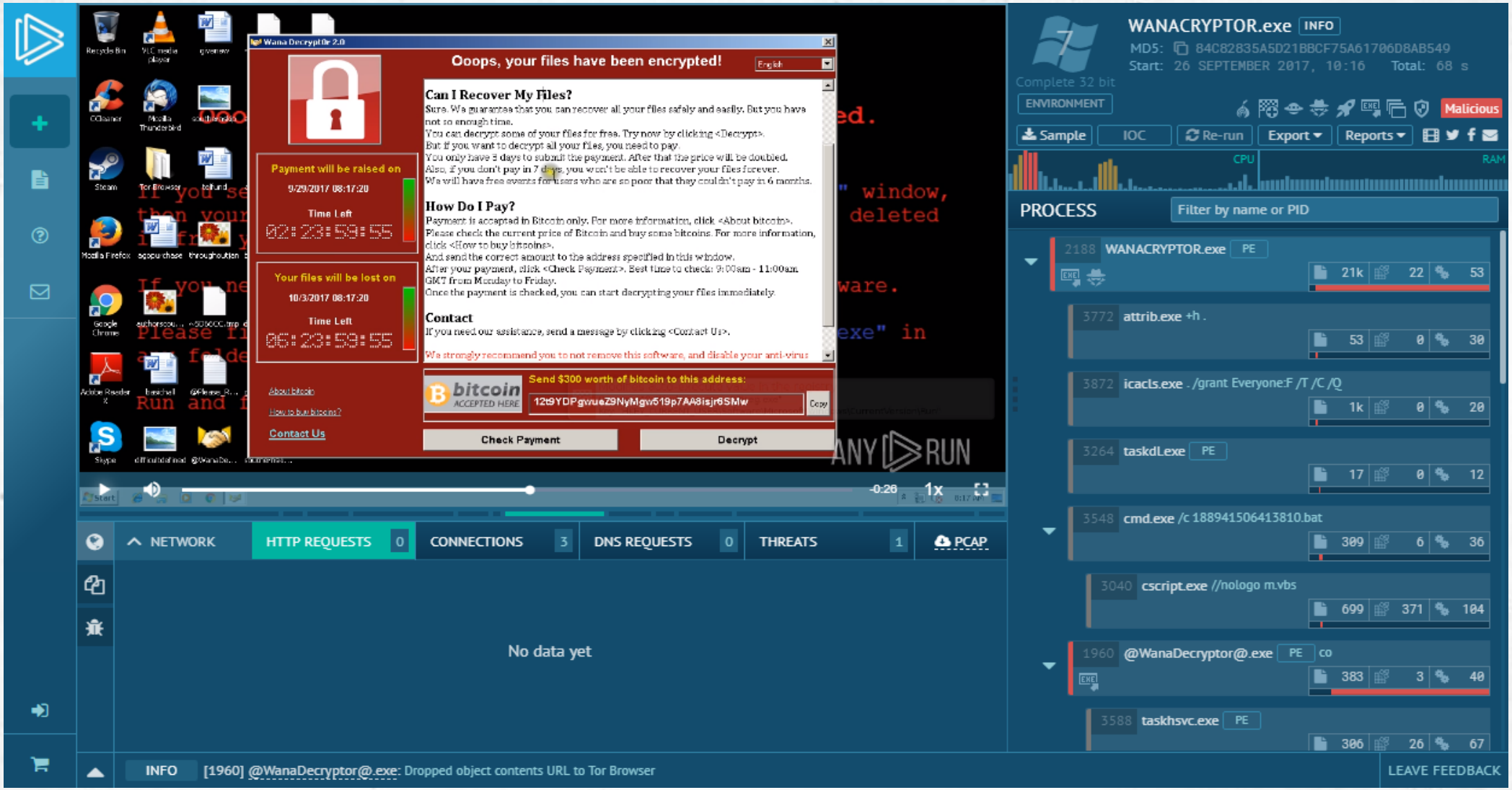
Zdroj: https://www.welivesecurity.com/wp-content/uploads/2016/03/Ton-Snoei-623x410.jpg

Distribúcia malvéru (IV.)



Zdroj: https://www.vdalabs.com/2017/11/27/modern-phishing-attack-part-1-malware-delivery/

AnyRun



Zdroj: https://any.run/

Typy malvéru (I.)

Rôzne typy:

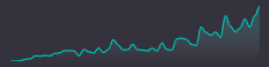
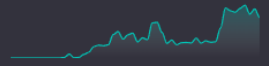
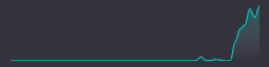
- Backdoor
- Bitcoin Miner / Stealer
- Click Fraud
- DoS
- Downloader / Dropper
- Ransomware
- Remote Access Tool
- …

Typy malvéru (II.)

MALWARE TRENDS TRACKER

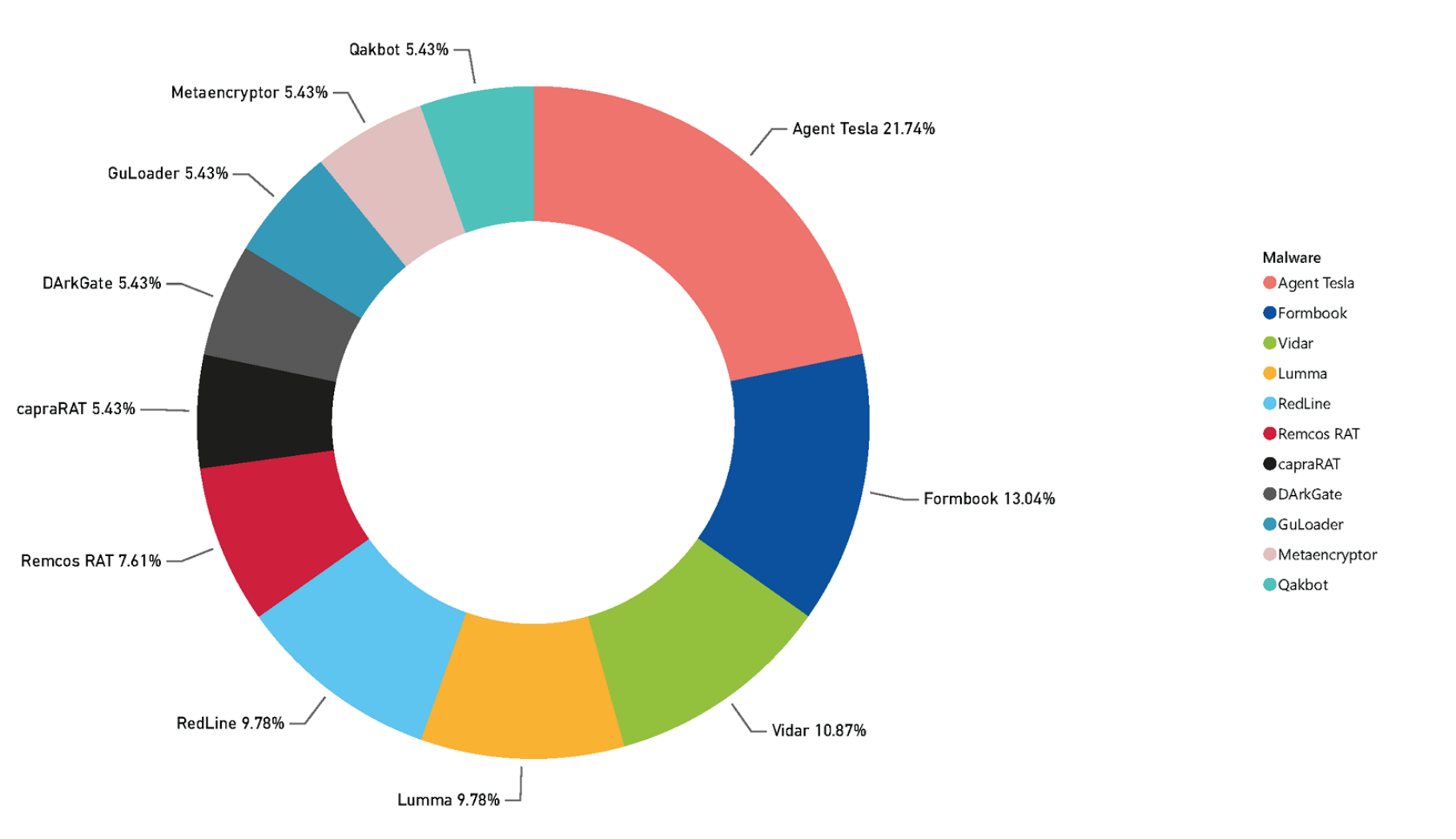
Most known malware from all over the cybersecurity world

Search by malware name...

No.	Family	Type	Trend changes	World rank	Tasks overall
1	Emotet	Trojan		1	115870
2	Tycoon 2FA	Phishingkit		2	94702
3	Agent Tesla	Trojan		3	50094
4	njRAT	Trojan		6	47984
5	RedLine	Stealer		7	45494
6	Lumma	Stealer		8	40656
7	Remcos	Trojan		10	37217
8	WannaCry	Ransomware		12	37151
9	AsyncRAT	RAT		13	36006
10	EvilProxy	Phishingkit		14	31362
11	Formbook	Spyware		15	27655

Zdroj: https://any.run/malware-trends/

Typy malvéru (III.)



Zdroj: ENISA Landscape 2024, https://www.enisa.europa.eu/publications/enisa-threat-landscape-2024

Vírus a červ (I.)

Vírus (virus)

- Pripojenie k rôznym programom a spustenie kódu
- Šírenie pomocou ľudskej aktivity (spustenie programu, otvorenie súboru)

Počítačový červ (computer worm)

- Zaťažujú počítačové siete alebo preťažujú sieťové služby
- Schopnosť samostatne sa replikovať a šíriť samostatne
- Príklad – Stuxnet – 2010 – Iránsky vládny program

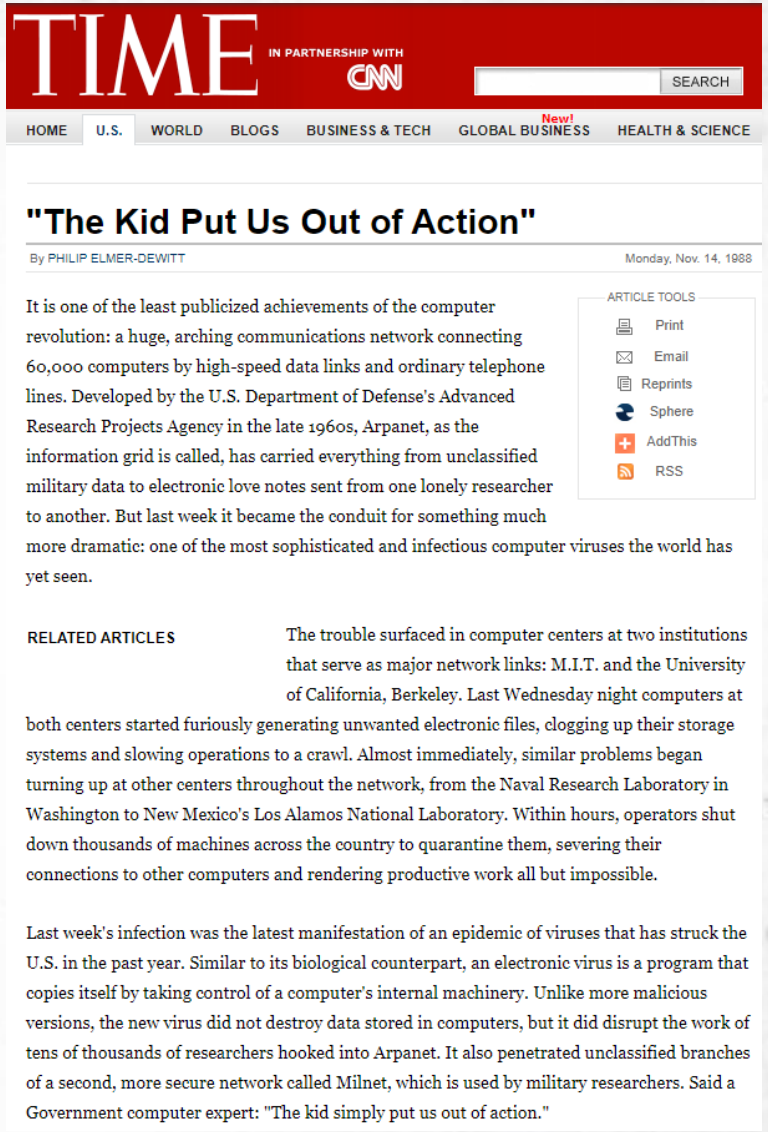
Zdroj: https://www.imdb.com/title/tt5446858/

Na počiatku bol červ (I.)

Zdroj: https://www.artstation.com/artwork/3r0VY

Na počiatku bol červ (II.)

- Okolo 20:30 hod. **2. novembra 1988** sa na internete z počítača na Massachusetts Institute of Technology (MIT) spustil zákerne šikovný program.
- Tento kybernetický červ sa čoskoro šíril pozoruhodnou rýchlosťou a zastavoval počítače.
- **Arpanet** - vyvinutý Agentúrou pre pokročilé výskumné projekty Ministerstva obrany USA koncom 60. rokov 20. storočia



TIME IN PARTNERSHIP WITH CNN

SEARCH

HOME | U.S. | WORLD | BLOGS | BUSINESS & TECH | GLOBAL BUSINESS (New!) | HEALTH & SCIENCE

"The Kid Put Us Out of Action"

By PHILIP ELMER-DEWITT — Monday, Nov. 14, 1988

ARTICLE TOOLS
Print
Email
Reprints
Sphere
AddThis
RSS

It is one of the least publicized achievements of the computer revolution: a huge, arching communications network connecting 60,000 computers by high-speed data links and ordinary telephone lines. Developed by the U.S. Department of Defense's Advanced Research Projects Agency in the late 1960s, Arpanet, as the information grid is called, has carried everything from unclassified military data to electronic love notes sent from one lonely researcher to another. But last week it became the conduit for something much more dramatic: one of the most sophisticated and infectious computer viruses the world has yet seen.

RELATED ARTICLES

The trouble surfaced in computer centers at two institutions that serve as major network links: M.I.T. and the University of California, Berkeley. Last Wednesday night computers at both centers started furiously generating unwanted electronic files, clogging up their storage systems and slowing operations to a crawl. Almost immediately, similar problems began turning up at other centers throughout the network, from the Naval Research Laboratory in Washington to New Mexico's Los Alamos National Laboratory. Within hours, operators shut down thousands of machines across the country to quarantine them, severing their connections to other computers and rendering productive work all but impossible.

Last week's infection was the latest manifestation of an epidemic of viruses that has struck the U.S. in the past year. Similar to its biological counterpart, an electronic virus is a program that copies itself by taking control of a computer's internal machinery. Unlike more malicious versions, the new virus did not destroy data stored in computers, but it did disrupt the work of tens of thousands of researchers hooked into Arpanet. It also penetrated unclassified branches of a second, more secure network called Milnet, which is used by military researchers. Said a Government computer expert: "The kid simply put us out of action."

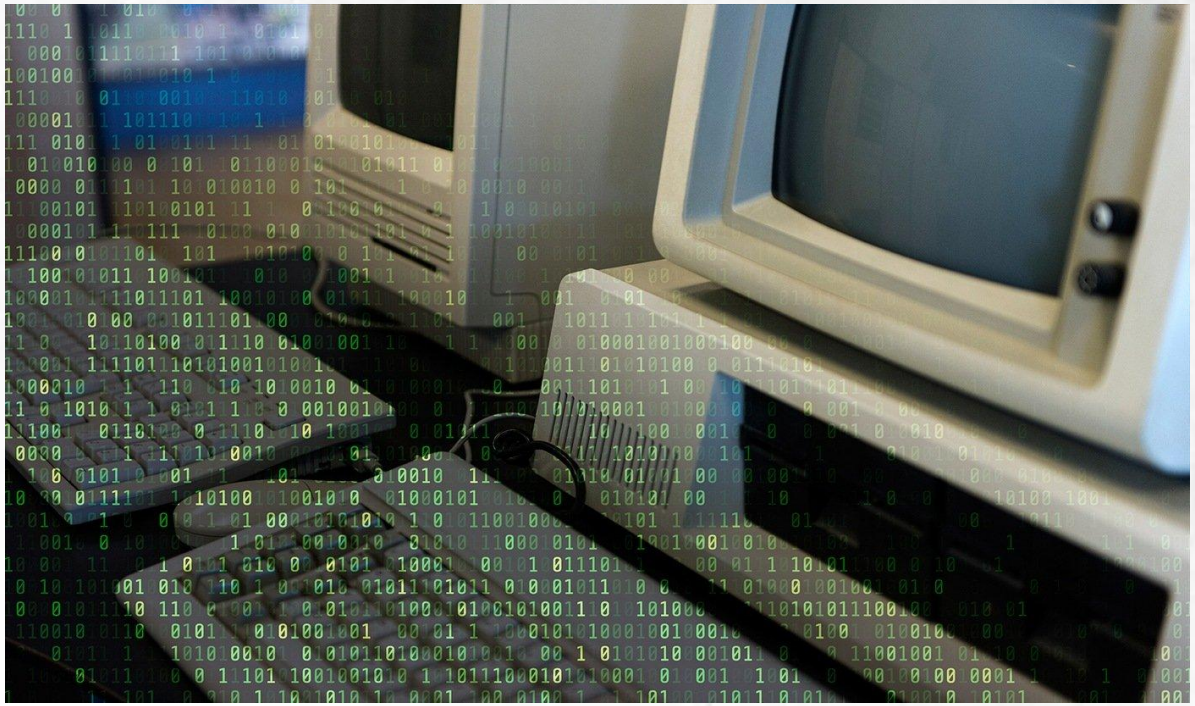
Zdroj: https://web.archive.org/web/20080206220309/http://www.time.com/time/magazine/article/0,9171,968884,00.html

Na počiatku bol červ (III.)

- "Momentálne sme pod útokom," napísal znepokojený študent Kalifornskej univerzity v Berkeley v e-maile neskôr v noci.

- „O 1:05 prenikol červ do Národného laboratória Lawrence Livermore National Laboratory, miesta zodpovedného za zabezpečenie jadrového arzenálu krajiny," napísal Shapiro vo Fancy Bear Goes Phishing.

- „Čoskoro sa červ zahrabal do Národného laboratória Los Alamos v Novom Mexiku, kde sa nachádzal projekt Manhattan a prvé atómové bomby na svete. Robertov geniálny projekt sa už nezdal taký geniálny."



Zdroj: https://www.fbi.gov/history/famous-cases/morris-worm

- **Do 24 hodín** bolo zasiahnutých odhadom 6 000 z približne 60 000 počítačov, ktoré boli vtedy pripojené na internet.

Na počiatku bol červ (IV.)

Červ sa šíril štyrmi mechanizmami:

- cez chybu v Sendmail,
- prostredníctvom chyby v programe Finger,
- prostredníctvom funkcie „dôveryhodných hostiteľov“, ktorá umožňuje používateľom z jedného systému používať iný systém bez hesla.
- cez heslo útok hrubou silou.


```
209
210     /* Collect hostnames and run hueristic #1 for this user's .forward and .rhosts
211      */
212     /* This is only called from try_passwd() */
213     static attack_user(user)                        /* 0x6514 */
214          struct usr *user;
215     {
216         FILE *fwd_fp;
217         char buf[512], *hostpart;                   /* 1516 */
218         char rhbuf[256];                            /* 1776 */
219         char l1288[512];
220         struct hst *host;                           /* 11292 */
```

```
87  static mainloop()                                   /* 0x2302 */
88  {
89      long key, time1, time0;
90
91      time(&key);
92      srandom(key);
93      time0 = key;
94      if (hg() == 0 && h1() == 0)
95          ha();
96      checkother();
97      report_breakin();
98      cracksome();
99      other_sleep(30);
100     while (1) {
101         /* Crack some passwords */
102         cracksome();
103         /* Change my process id */
104         if (fork() > 0)
105             exit(0);
106         if (hg() == 0 && hi() == 0 && ha() == 0)
107             h1();
108         other_sleep(120);
109         time(&time1);
110         if (time1 - time0 >= 60*60*12)
111             h_clean();
112         if (pleasequit && nextw > 0)
113             exit(0);
114     }
115 }
```

Zdroj: https://www.artstation.com/artwork/3r0VY

Na počiatku bol červ (V.)

- **Robert Tappan Morris**
- Dostal pokutu 10.050 $, 400 hodín verejnoprospešných prác a trojročnú podmienku.
- Odhadovalo sa, že na vyčistenie po červovi bolo na infikované zariadenie potrebných 200 až 53.000 $.

928 F.2d 504 (1991)

UNITED STATES of America, Appellee,
v.
Robert Tappan MORRIS, Defendant-Appellant.

No. 774, Docket 90-1336.

United States Court of Appeals, Second Circuit.

Argued December 4, 1990.
Decided March 7, 1991.

Thomas A. Guidoboni, Washington, D.C., for defendant-appellant.

Ellen R. Meltzer, U.S. Dept. of Justice, Washington, D.C. (Frederick J. Scullin, Jr., U.S. Atty., Syracuse, N.Y., Mark D. Rasch, U.S. Dept. of Justice, Washington, D.C., on the brief), for appellee.

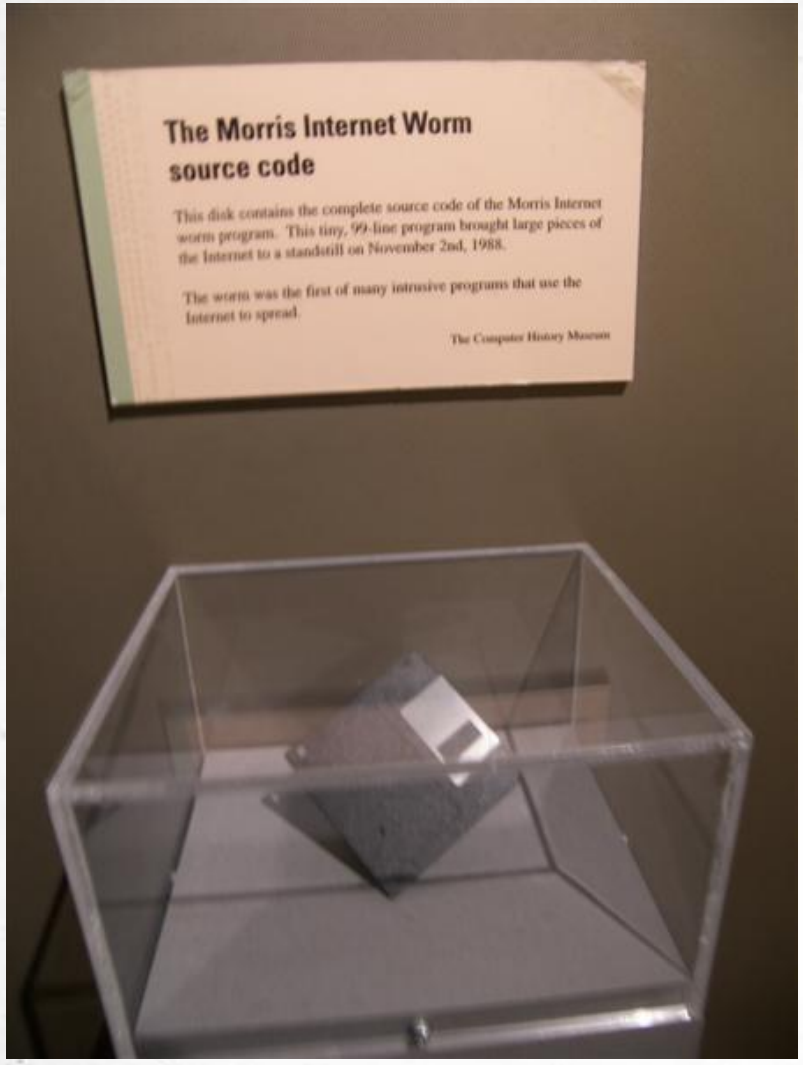
*505 Before NEWMAN and WINTER, Circuit Judges, and DALY, District Judge.[*]

JON O. NEWMAN, Circuit Judge:

This appeal presents two narrow issues of statutory construction concerning a provision Congress recently adopted to strengthen protection against computer crimes. Section 2(d) of the Computer Fraud and Abuse Act of 1986, 18 U.S.C. § 1030(a)(5)(A) (1988), punishes anyone who intentionally accesses without authorization a category of computers known as "[f]ederal interest computers" and damages or prevents authorized use of information in such computers, causing loss of $1,000 or more. The issues raised are (1) whether the Government must prove not only that the defendant intended to access a federal interest computer, but also that the defendant intended to prevent authorized use of the computer's information and thereby cause loss; and (2) what satisfies the statutory requirement of "access without authorization."

Zdroj: https://scholar.google.com/scholar_case?case=551386241451639668

Na počiatku bol červ (VI.)



PI CORE/DUAL

Robert Morris

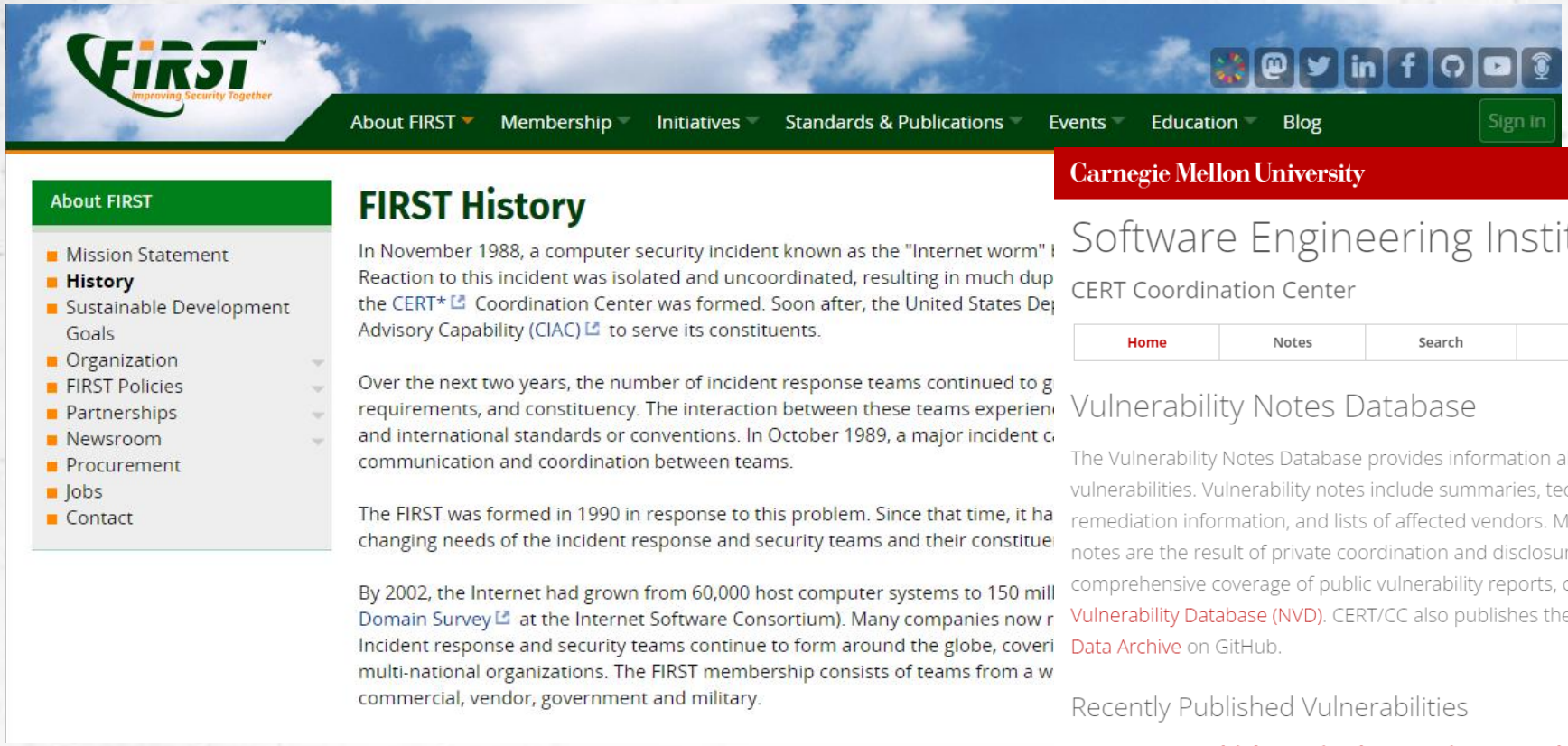
Professor

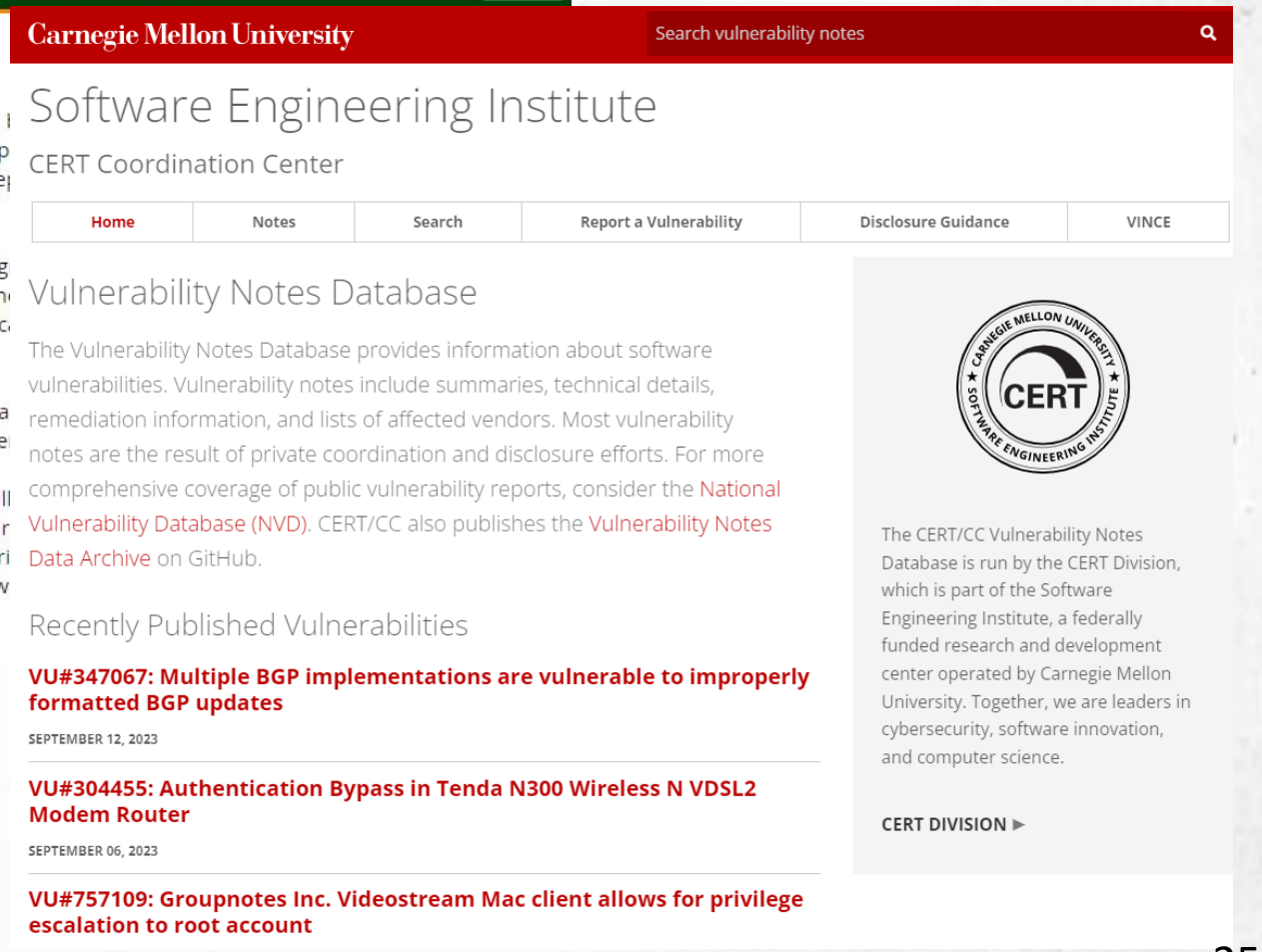
EMAIL	PHONE	ROOM
rtm@csail.mit.edu	253-5983	32-G972

Robert Morris is a professor in MIT's EECS department and a member of the Computer Science and Artificial Intelligence Laboratory. He received a PhD from Harvard University for work on modeling and controlling networks with large numbers of competing connections. As a graduate student he helped design and build an ARPA-funded ATM switch with per-circuit hop-by-hop flow control. He led a mobile communication project which won a best student paper award from USENIX. He co-founded Viaweb, an e-commerce hosting service. His current interests include modular software-based routers, analysis of the aggregation behavior of Internet traffic, and scalable ad-hoc routing.

Zdroj: https://en.wikipedia.org/wiki/Morris_worm#/media/File:Morris_Worm.jpg, https://www.csail.mit.edu/person/robert-morris

Na počiatku bol červ (VII.)





Zdroj: https://www.kb.cert.org/vuls/, https://www.first.org/about/history

Trojský kôň (I.)

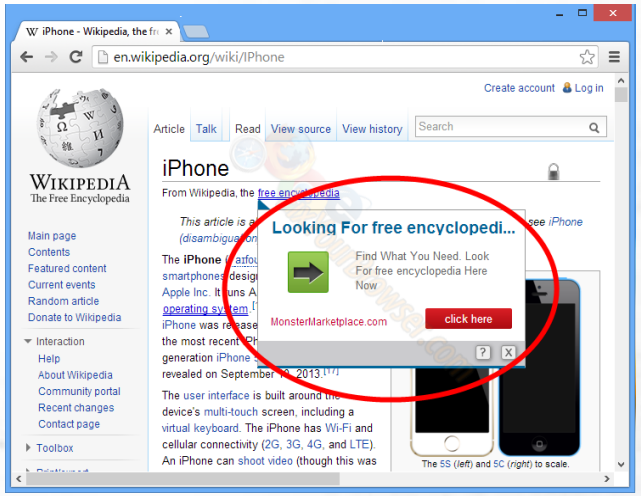
Trojský kôň

- Umožňuje iným osobám vzdialený prístup k infikovanému zariadeniu
- Zvukové alebo video doplnky (plug-iny) šírenie pomocou ľudskej aktivity (spustenie programu, otvorenie súboru)

CCleaner 5.33.6162

Adware

- Automaticky poskytuje reklamu
- Napr. pop-up reklamy na webových stránkach



Zdroj: https://commons.wikimedia.org/wiki/File:Trojan-Horse-Virus-Remover.png, https://sensorstechforum.com/ccleaner-trojan-nyetya-malware-remove/

Trojský kôň (II.)

Nanocore

nanocore trojan rat loader

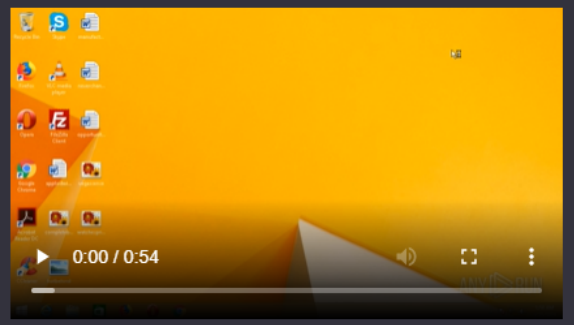
NanoCore is a Remote Access Trojan or RAT. This malware is highly customizable with plugins which allow attackers to tailor its functionality to their needs. Nanocore is created with the .NET framework and it's available for purchase for just $25 from its "official" website.

Type
Trojan

Origin
USA

First seen
1 January, 2013

Last seen
3 December, 2020



Global rank	Week rank	Month rank	IOCs
4	↓5	↑5	8857

LAST SEEN AT

3 December, 2020	Malicious activity	dfgn.exe	rat nanocore trojan
3 December, 2020	Malicious activity	dfgn.exe	rat nanocore trojan
3 December, 2020	Malicious activity	dfgn.exe	rat nanocore trojan
3 December, 2020	Malicious activity	adsense_setup.exe	rat nanocore trojan
3 December, 2020	Malicious activity	joshrat.exe	rat nanocore trojan

Zdroj: https://any.run/malware-trends/nanocore, https://app.any.run/tasks/454b93d0-08bc-400c-8c66-0fd6980bce6a/

Spyware (I.)

Spyware

- Sleduje aktivity používateľa bez jeho vedomia a zhromažďuje o ňom údaje

Keylogger

- Zaznamenáva všetko, čo používateľ zadá na svojom zariadení
- Napr. prihlasovacie mená, heslá a ďalšie citlivé údaje
- 2 typy - softvérové a hardvérové keyloggery

Spyware (II.)

Agent Tesla

agenttesla trojan rat stealer

Agent Tesla is spyware that collects information about the actions of its victims by recording keystrokes and user interactions. It is falsely marketed as a legitimate software on the dedicated website where this malware is sold.

Type
Trojan

Origin
Likely Turkey

First seen
1 January, 2014

Last seen
3 December, 2020

Global rank	Week rank	Month rank	IOCs
2	↑4	↓4	17795

LAST SEEN AT

3 December, 2020	Malicious activity	400000.Payment advise_pdf_____.exe	rat agenttesla trojan
3 December, 2020	Malicious activity	Payment advise_pdf_____.exe	rat agenttesla
3 December, 2020	Malicious activity	company details.pps	macros macros-on-close rat agenttesla trojan stealer

Zdroj: https://any.run/malware-trends/agenttesla, https://app.any.run/tasks/f5c4395c-3a53-47c8-9481-29caa2734c77/

Ransomvér (I.)

Ransomvér

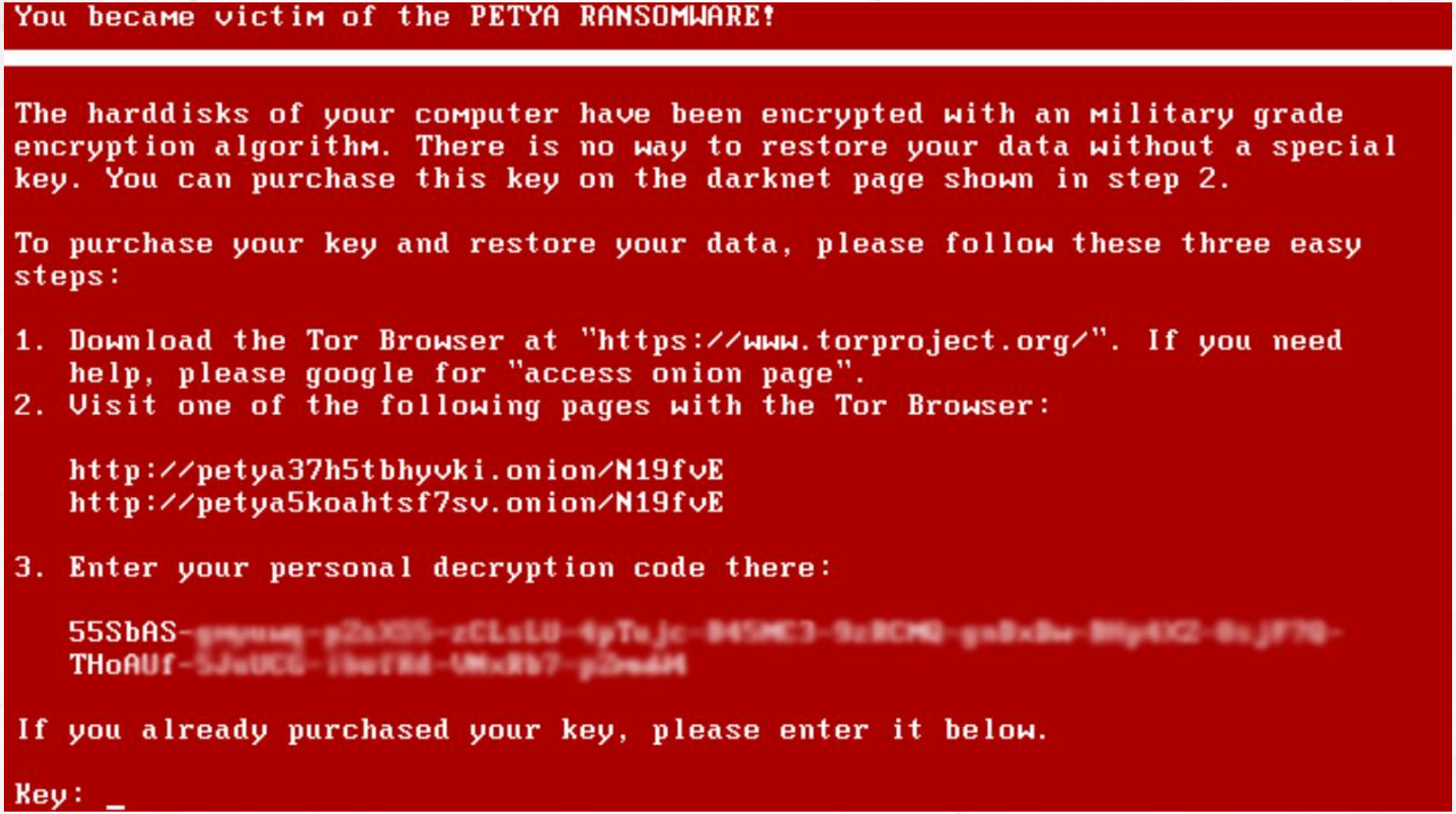
- Šifrovanie údajov
- Výkupne - BitCoin
- Zablokovanie PC
- Nemožnosť dešifrovať dáta
- Mazanie súborov
- Slabá ochrana
- Zálohovanie
- Známe príklady – Locky, Petya, Goldeneye

Incidents

- The Baltimore County incident[1]
- Alabama hospitals attack[7]
- Lodi California City incident[4]
- Texas (Texas Department of Information Resources) incident[5]
- Lake City (Florida) Ryuk attack[2]
- New Belford (Massachusetts) incident[6]
- Ransomware attacks on > 500 schools and universities[8]
- Wood Ranch Medical (California) case[12]
- Michigan Brookside ENT and Hearing Centre incident[13]
- Gippsland Health Alliance and the South West Alliance of Rural Health (Australia) incidents[14]
- Premier Family Medical group (Utah) incident[15]
- MSPs PM Consultants, CloudJumper, Datto, PercSoft, TSM Consulting Services Inc. and IT By Design incidents[19]
- Microsoft Azure data centre incident[51]
- Altran Technologies LockerGoga attack[40]
- Norsk Hydro LockerGoga attack[7]
- Hexion and the Momentive LockerGoga attacks[41]
- Albany IT incident[60]
- Jackson County (Georgia) incident[61]
- Riviera Beach (Florida) incident[62]
- New Orleans incident[63]
- Danish hearing aid manufacturer Demant attack[64]

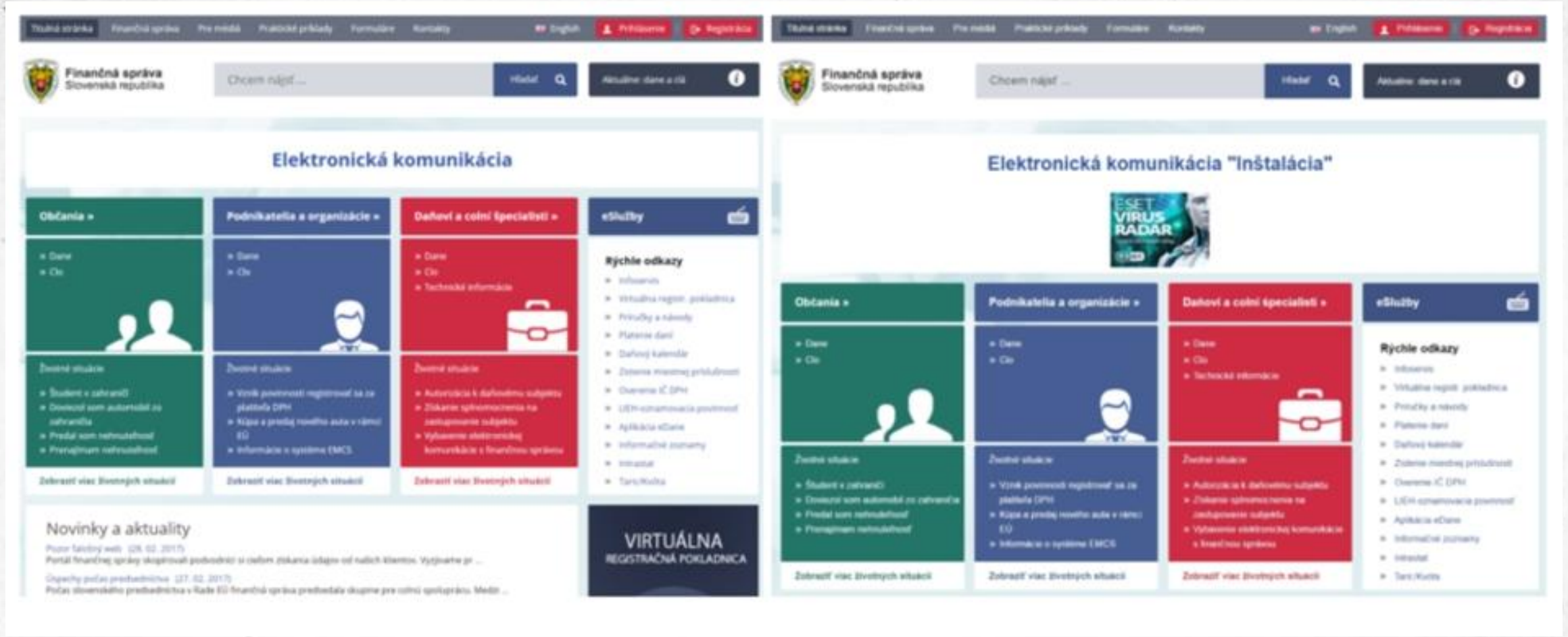
Zdroj: ENISA Threat Landscape 2020, ENISA, 2021.

Ransomvér (II.)



https://krebsonsecurity.com/2017/06/petya-ransomware-outbreak-goes-global/

Ransomvér (III.)

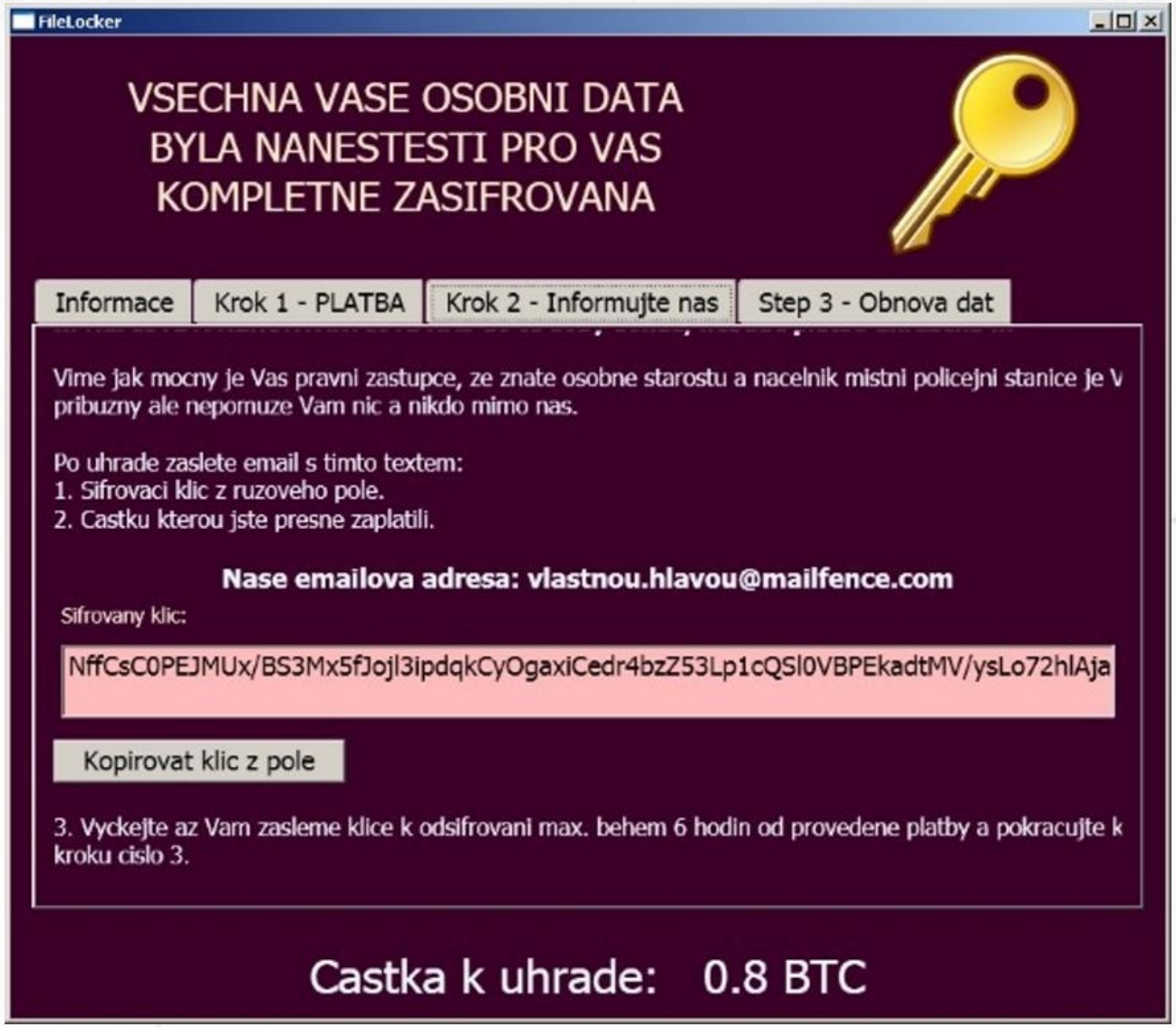


Skutočné webové sídlo Finančnej správy

Falošné webové sídlo www.financnasprava.digital

Zdroj: https://touchit.sk/skodlivy-kod-zneuzivajuci-financnu-spravu-ziada-vykupne-900-eur-peniaze-pyta-vlastnou-hlavou/101911

Ransomvér (IV.)



Zdroj: https://touchit.sk/skodlivy-kod-zneuzivajuci-financnu-spravu-ziada-vykupne-900-eur-peniaze-pyta-vlastnou-hlavou/101911

Ransomvér (V.)

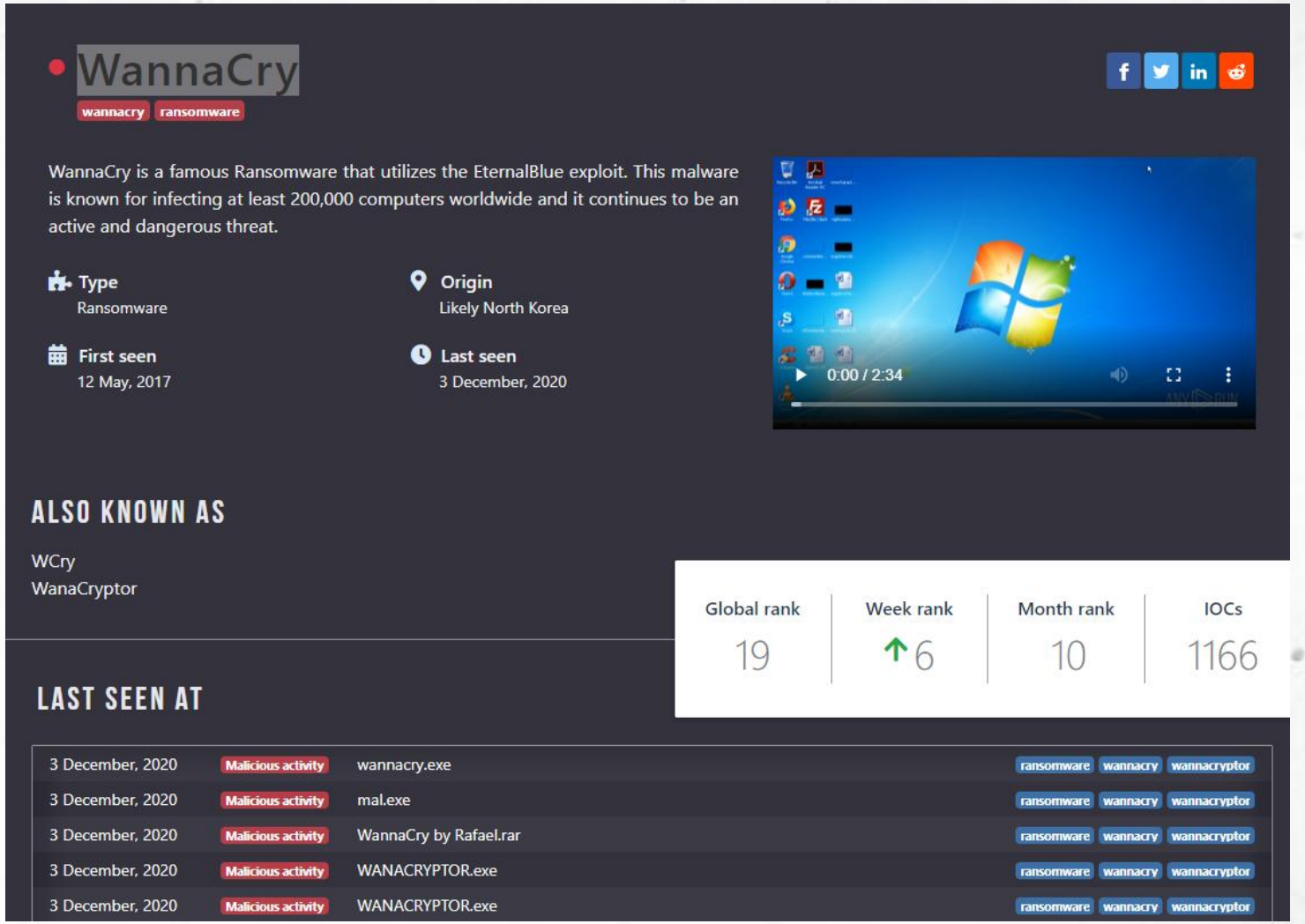
Email: servis@financnasprava.digital

0,8 B = cca 900€

Dodatok:
“I nám jde o profesionální klientský servis a reputaci na trhu, proto se budeme snažit odemknout Vaše soubory co nejdříve”

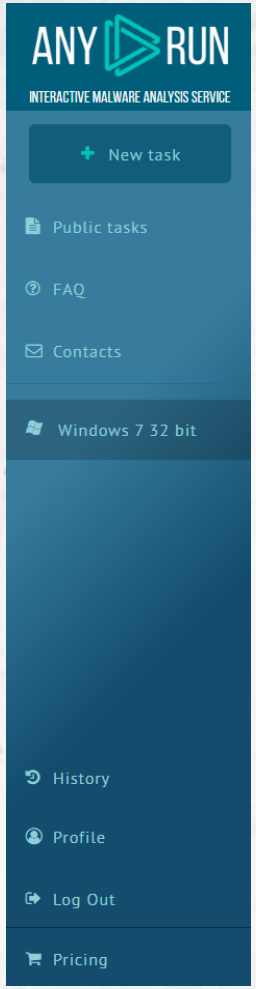
Zdroj: https://touchit.sk/skodlivy-kod-zneuzivajuci-financnu-spravu-ziada-vykupne-900-eur-peniaze-pyta-vlastnou-hlavou/101911

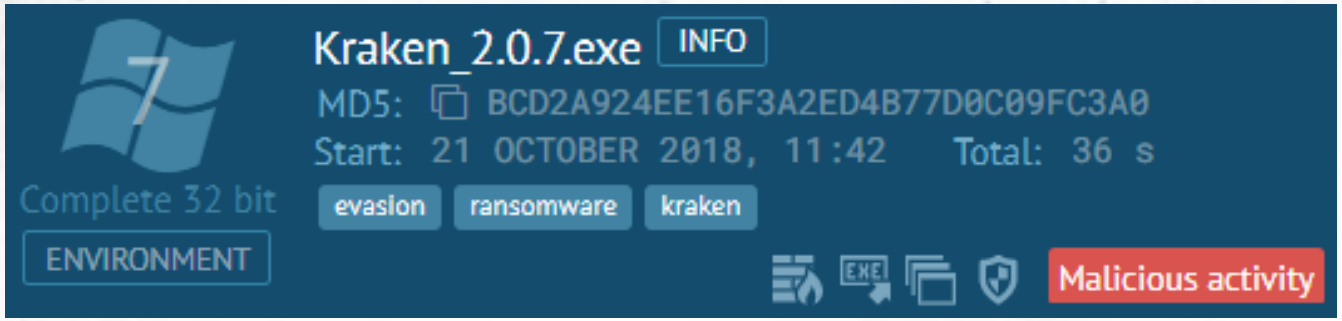
Ransomvér (VI.)



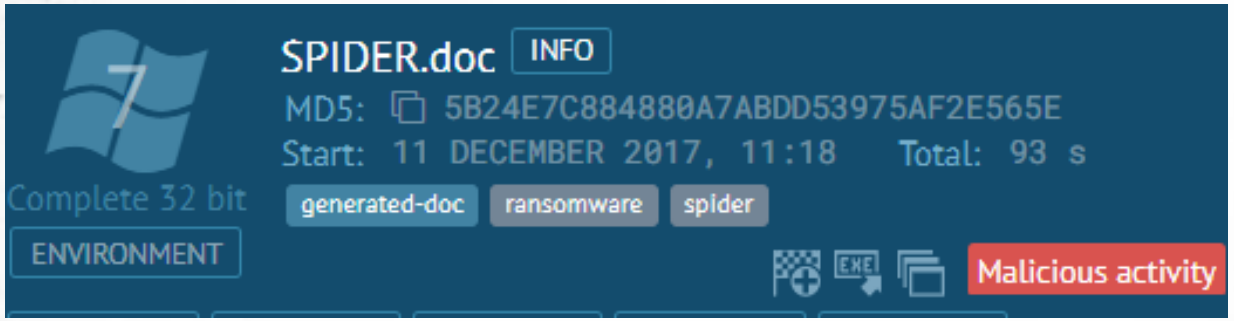
Zdroj: https://any.run/malware-trends/wannacry

Ransomvér (VII.)





https://app.any.run/tasks/32186bb2-60c2-4980-8bf8-4b2742697df4/



https://app.any.run/tasks/997c3dc0-b14e-441c-a4b3-c952718dc9fc/

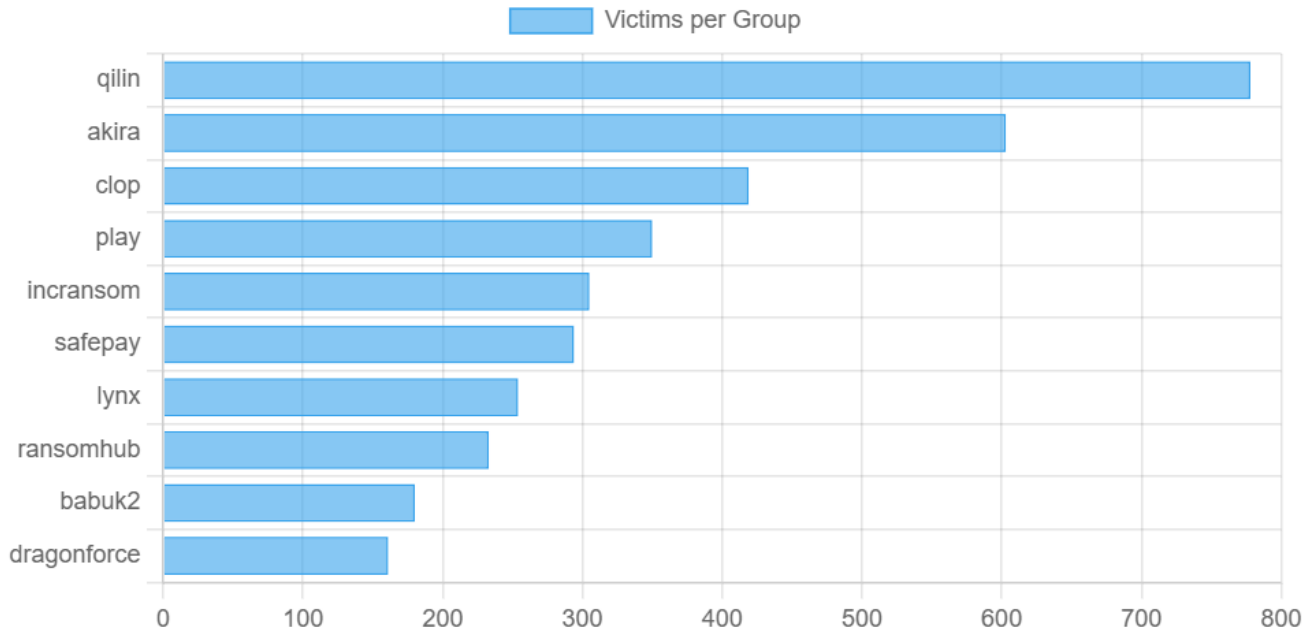
Ransomvér (VIII.)

Ransomware Statistics for 2025

Total Victims for 2025: 6620

Total Groups: 297

Top 10 Groups



Zdroj: https://www.ransomware.live/stats

Ransomvér (IX.)

All ransomware notes by groups

Note

> Ransomware notes are provided by Zscaler ThreatLabz under MIT License

8base	abysslocker	akira	alphv	atomsilo	avaddon	avoslocker	azov	beast	bianlian
biglock	bitpaymer	bitransomware	blackbasta	blackbyte	blackhunt	blackmatter	blacksnake	blacksuit	bluesky
cactus	cartel	cerber	chilelocker	cloak	clop	conti	cryptnet	cryptomix	cryptxxx
crytox	ctblocker	cuba	dagonlocker	darkangels	darkbit	darkpower	darkside	dataleak	deadbydawn
dharma	diavol	donut	doppelpaymer	dragonforce	ech0raix	esxiargs	ftcode	gandcrab	grief
gwisinlocker	h0lygh0st	hades	hive	hunters	icefire	inc	incransom	jaff	karakurt
karma	knight	lapiovra	lilith	lockbit	locky	lorenz	luckbit	lv	magniber
makop	mallox	maze	medusa	medusalocker	moneymessage	monti	nefilim	nemty	netwalker
nevada	noescape	nokoyawa	noname	novagroup	phobos	play	prometheus	qilin	qlocker
quantumlocker	ragnarlocker	ragnarok	rancoz	ransomexx	ransomhouse	ransomhub	ranzy	raworld	redalert
relic	revil	rhysida	rook	royal	rtmlocker	ryuk	scarecrow	schoolboys	shadow
slug	snatch	stop	sugar	suncrypt	teslacrypt	trigona	u-bomb	underground	vicesociety
vohuk	wastedlocker	xorist	yanluowang	zeon					

ast update : *Thursday 14/03/2024 20.59 (UTC)*

Zdroj: https://www.ransomware.live/

Ransomvér (X.)

Ransom notes for group play

play

- ReadMe.txt

```
PLAY
news portal, tor network links:
mbrlkbtq5jonaqkurjwmxftytyn2ethqvbxfu4rgjbkkknndqwae6byd.onion
k7kg3jqxang3wh7hnmaiokchk7qoebupfgoik6rha6mjpzwupwtj25yd.onion
derdiarikucisv@gmx.de
```

- play.txt

```
PLAY
teilightomemaucd@gmx.com
```

Ransom notes for group medusa

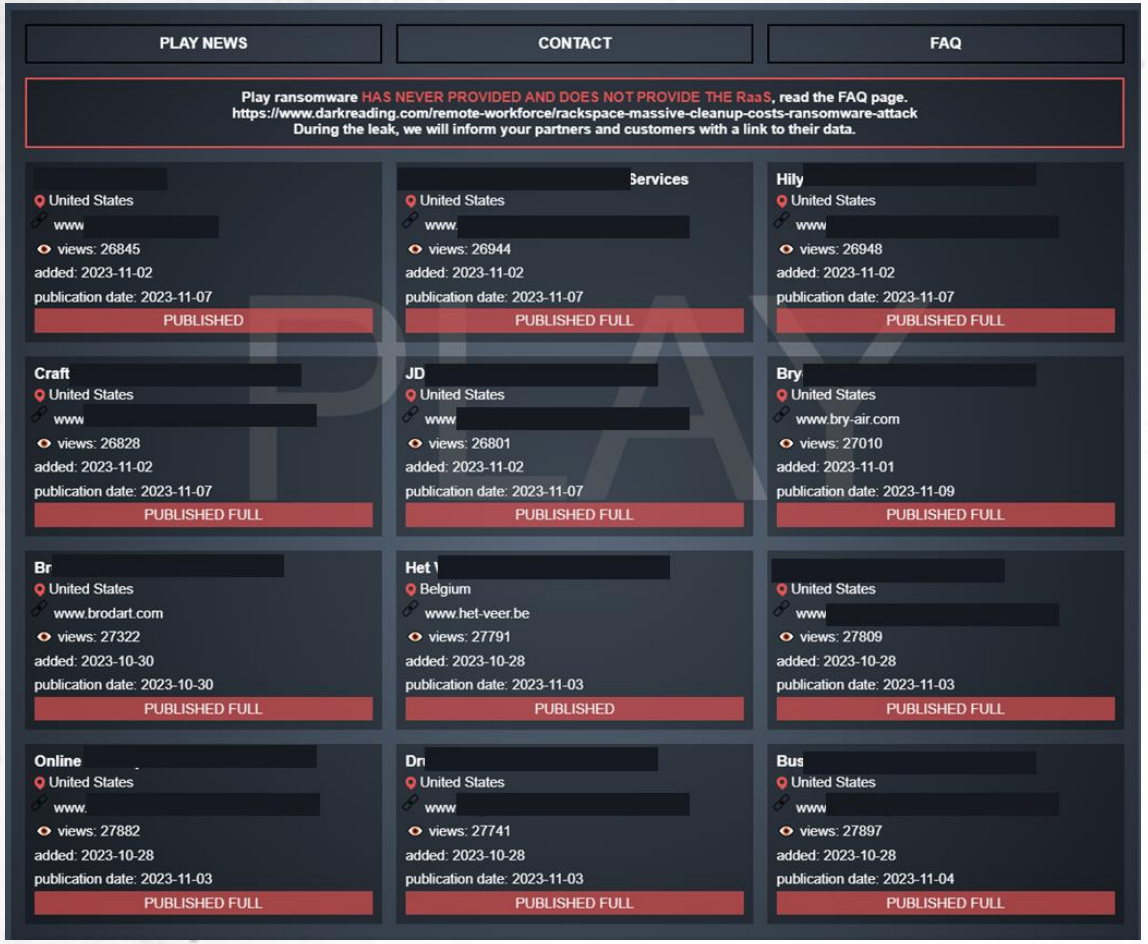
medusa medusa

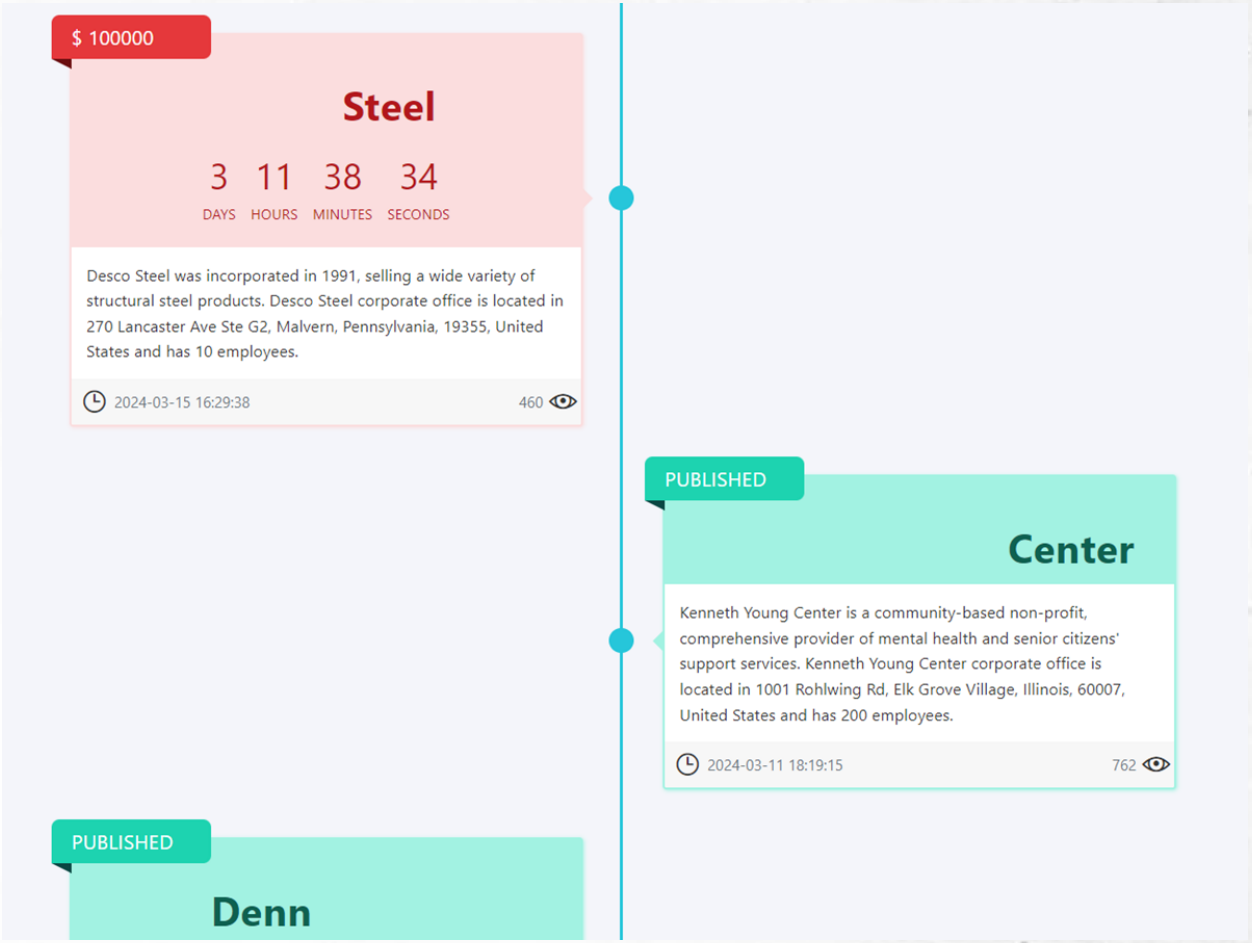
- !!!READ_ME_MEDUSA!!!.txt

```
$$\      $$\ $$$$$$$$\ $$$$$$$\  $$\   $$\  $$$$$$\   $$$$$$\
$$$\    $$$ |$$  _____|$$  __$$\ $$ |  $$ |$$  __$$\ $$  __$$\
$$$$\  $$$$ |$$ |      $$ |  $$ |$$ |  $$ |$$ /  \__|$$ /  $$ |
$$\$$\$$ $$ |$$$$$\    $$ |  $$ |$$ |  $$ |\$$$$$$\  $$$$$$$$ |
$$ \$$$  $$ |$$  __|   $$ |  $$ |$$ |  $$ | \____$$\ $$  __$$ |
$$ |\$  /$$ |$$ |      $$ |  $$ |$$ |  $$ |$$\   $$ |$$ |  $$ |
$$ | \_/ $$ |$$$$$$$$\ $$$$$$$  |\$$$$$$  |\$$$$$$  |$$ |  $$ |
\__|     \__|\________|\_______/  \______/  \______/ \__|  \__|
----------------------------[ Hello, [snip] !!! ]-------------------------

WHAT HAPPEND?
-------------------------------------------------------------
1. We have PENETRATE your network and COPIED data.
* We have penetrated entire network including backup system and researched all about your data.
* And we have extracted all of your networks including sub offices and your service clients networks valual

2. We have ENCRYPTED some your files.
While you are reading this message, it means you found your files and data has been ENCRYPTED by world's st
We have access to all of your sub offices and client service networks but didn't lock them all for your bra
We can solve this issue sliently and smoothly without 3rd parties and we decided lock only some of your ma
But don't worry, we can restore everything to the original without harming your business.

There is only one possible way to get back your systems and business - CONTACT us via LIVE CHAT and pay fo
MEDUSA DECRYPTOR and DECRYPTION KEYs, Data deletion, Keep silent in media.
This MEDUSA DECRYPTOR will restore your entire network, This will take less than 1 business day.
```

Zdroj: https://www.ransomware.live/

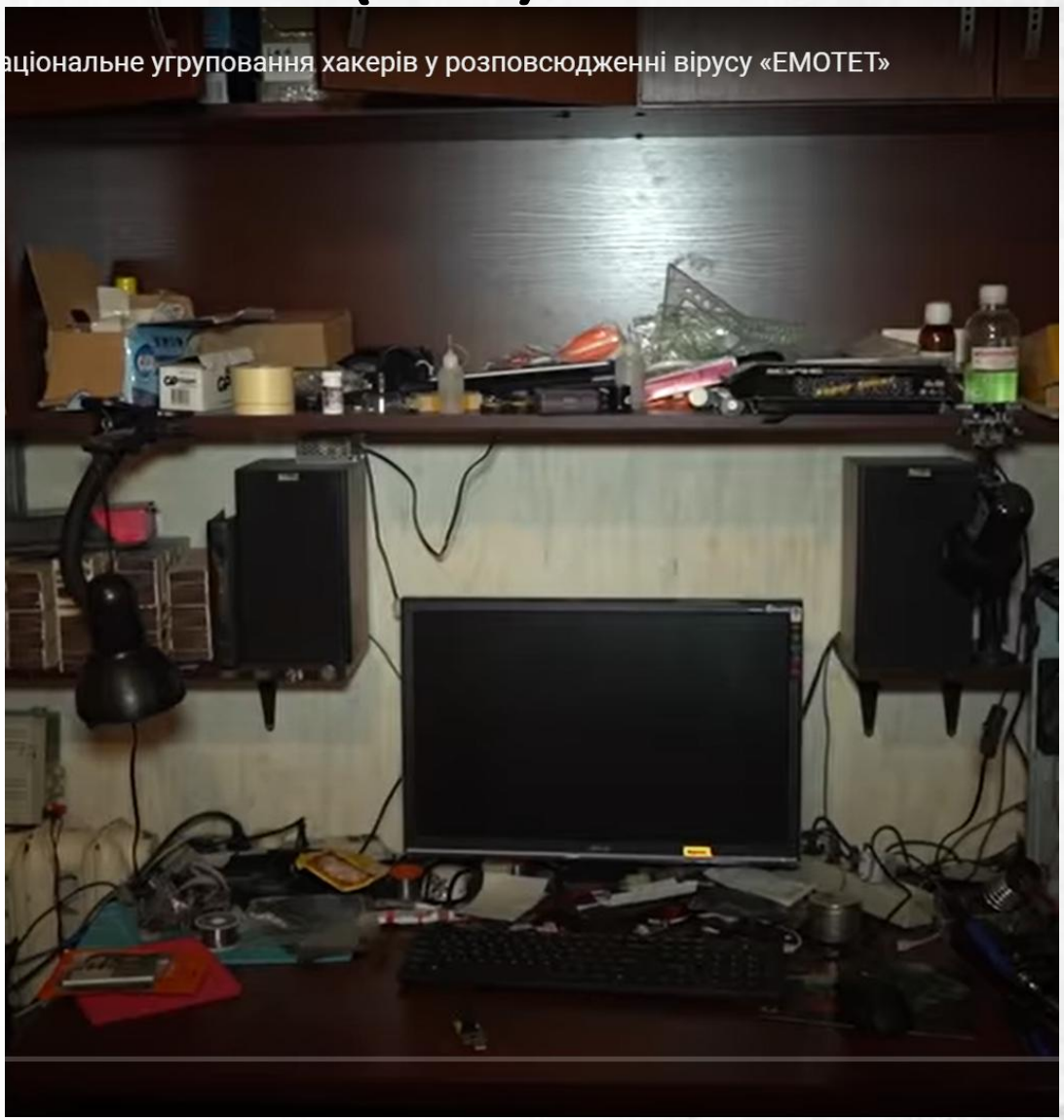
Ransomvér (XI.)





Ransomvér (XII.)

Medzinárodný policajný tím rozvrátil notoricky známy botnet Emotet



Zdroj: cybersec.sk/spravy/zo-sveta/medzinarodny-policajny-tim-rozvratil-notoricky-znamy-botnet-emotet/

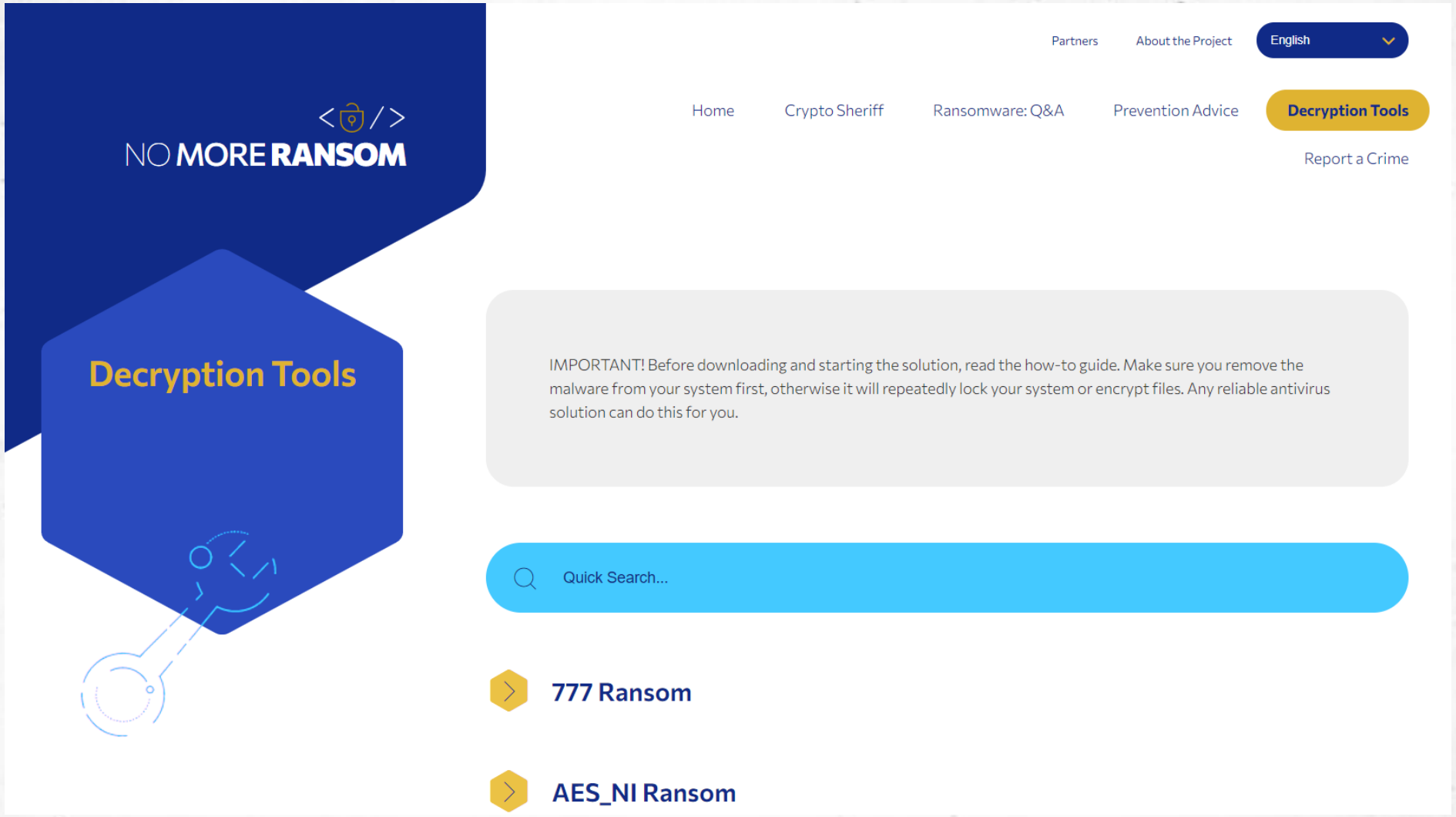
Ochrana voči malvéru

- Ochrana zariadení pripájajúcich sa do viacerých sietí

- Antivírusový program
- Nastavenia operačného systému
- Pripojenie do siete organizácie cez VPN

Dekryptor

https://www.nomoreransom.org/



Detekcia malvéru

Podľa signatúry

- porovnanie voči signatúre známych vzoriek
- malá chybovosť, ale nedeteguje neznáme vzorky

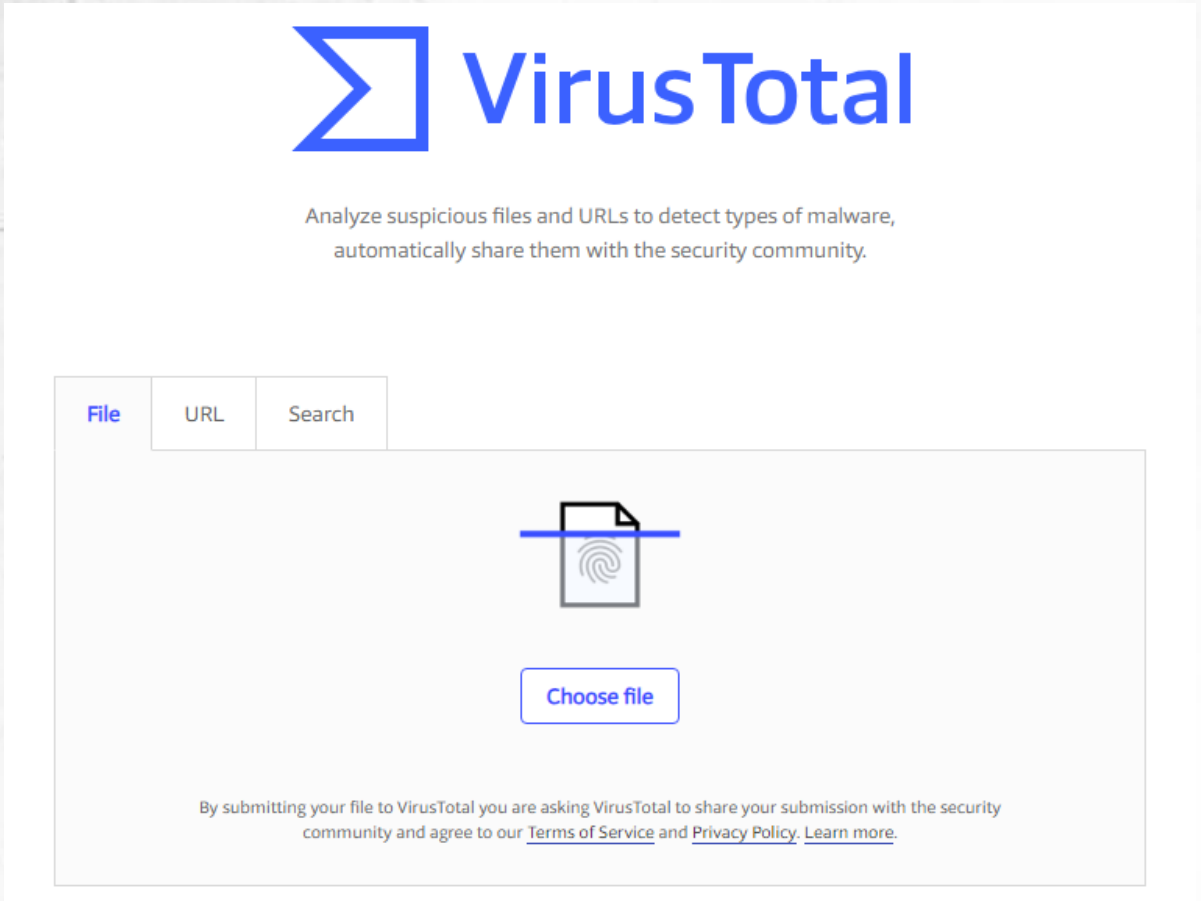
Podľa správania

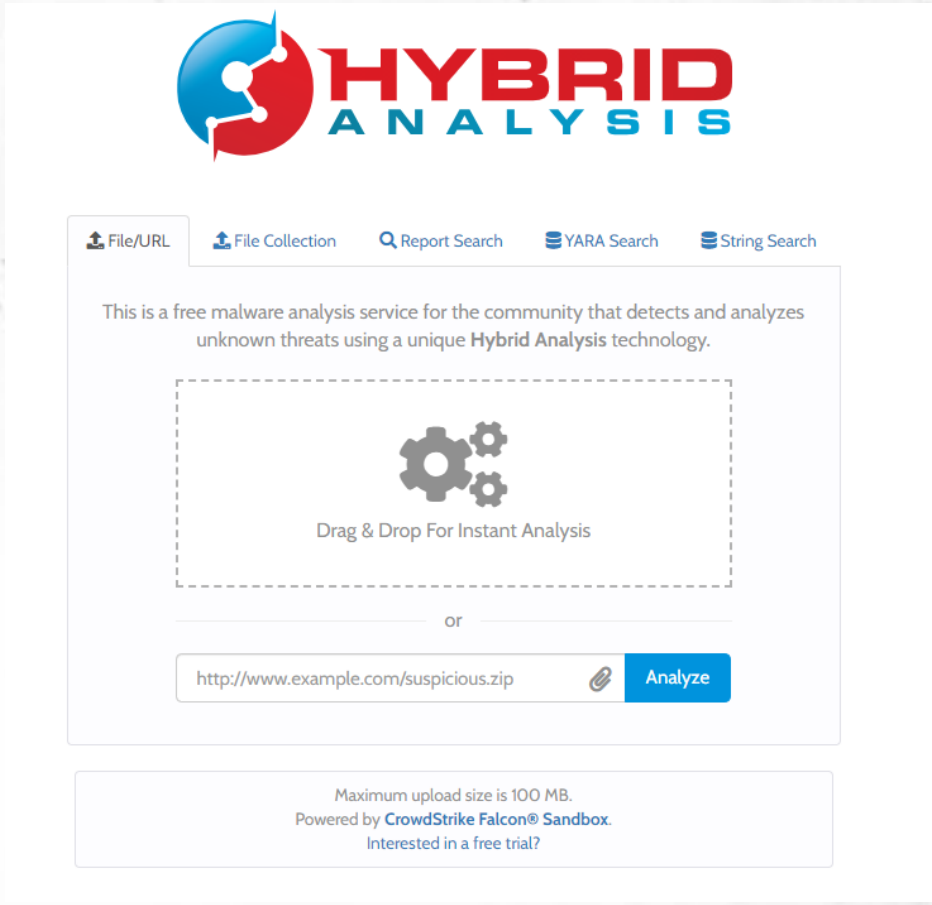
- podľa používaných systémových zdrojov sa rozhodne, či pôjde o malvér
- detekcia nových a mutujúcich typov

Podľa heuristiky

- na klasifikáciu, či ide o malvér, sa používa strojové učenie (machine learning)

Nástroje

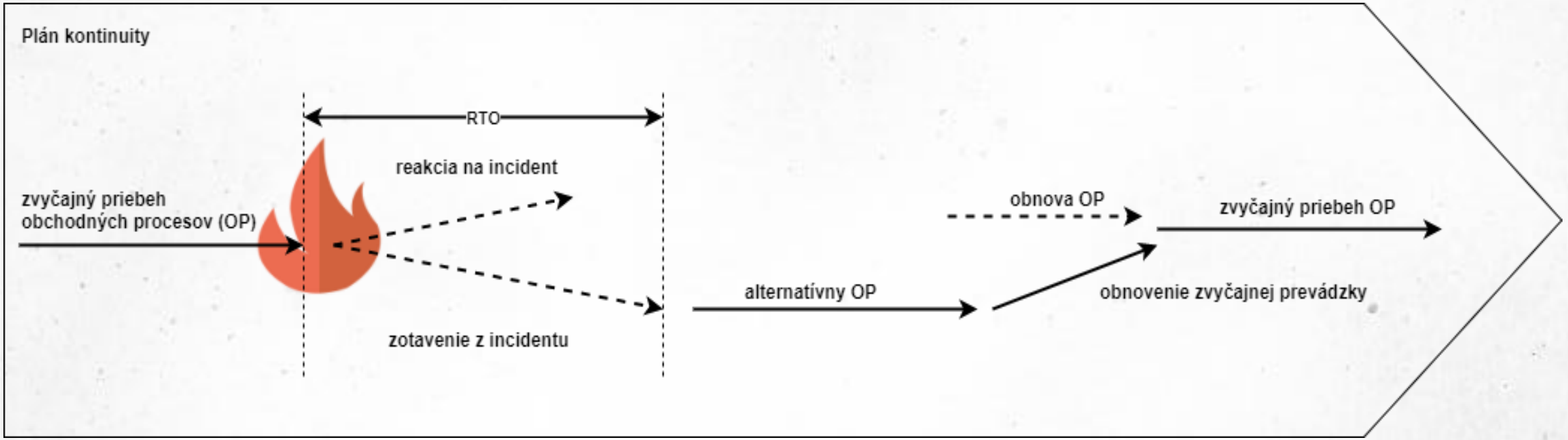




Príklady: https://hybrid-analysis.com/sample/c378387344e0a552dc065de6bfa607fd26e0b5c569751c79fbf9c6f2e91c9807?environmentId=100
https://www.virustotal.com/gui/file/4b59512ff60f7f88b05642f1c8ce012373af7d04a92196e2a5dc28213cfff4f7
https://www.virustotal.com/gui/file/de5b8737e4b7da9845901ecb8958e8d509507664de9dda76111795fdc60f0c86

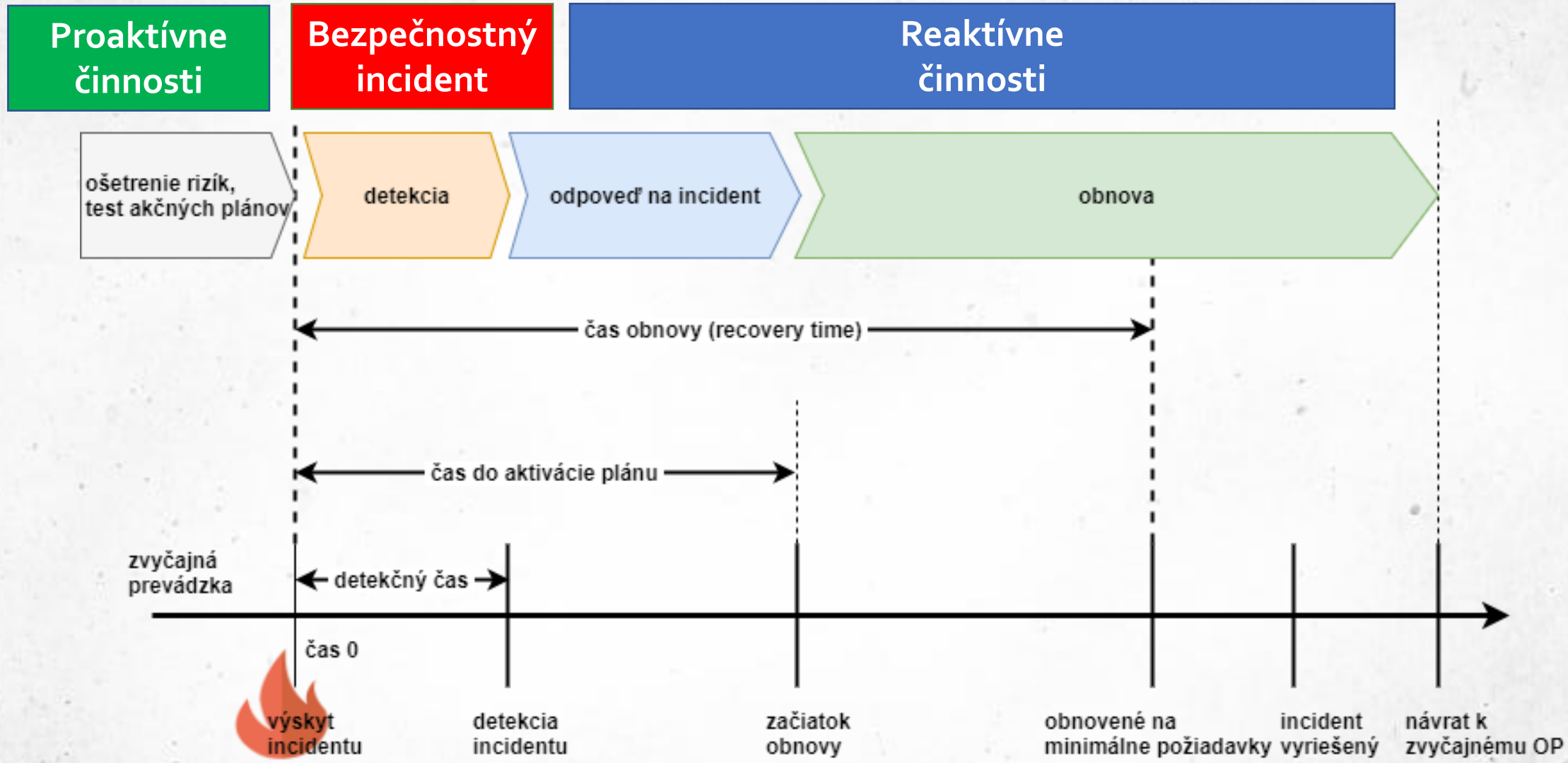
Kontinuita činností (I.)

- *schopnosť organizácie pokračovať v dodávke produktov a služieb v prijateľných časových rámcoch pri vopred definovanej kapacite počas narušenia* (ISO/IEC 22301:2019)



Zdroj: ISO/IEC 270035:2011

Kontinuita činností (II.)



Kontinuita činností (III.)

Prevencia

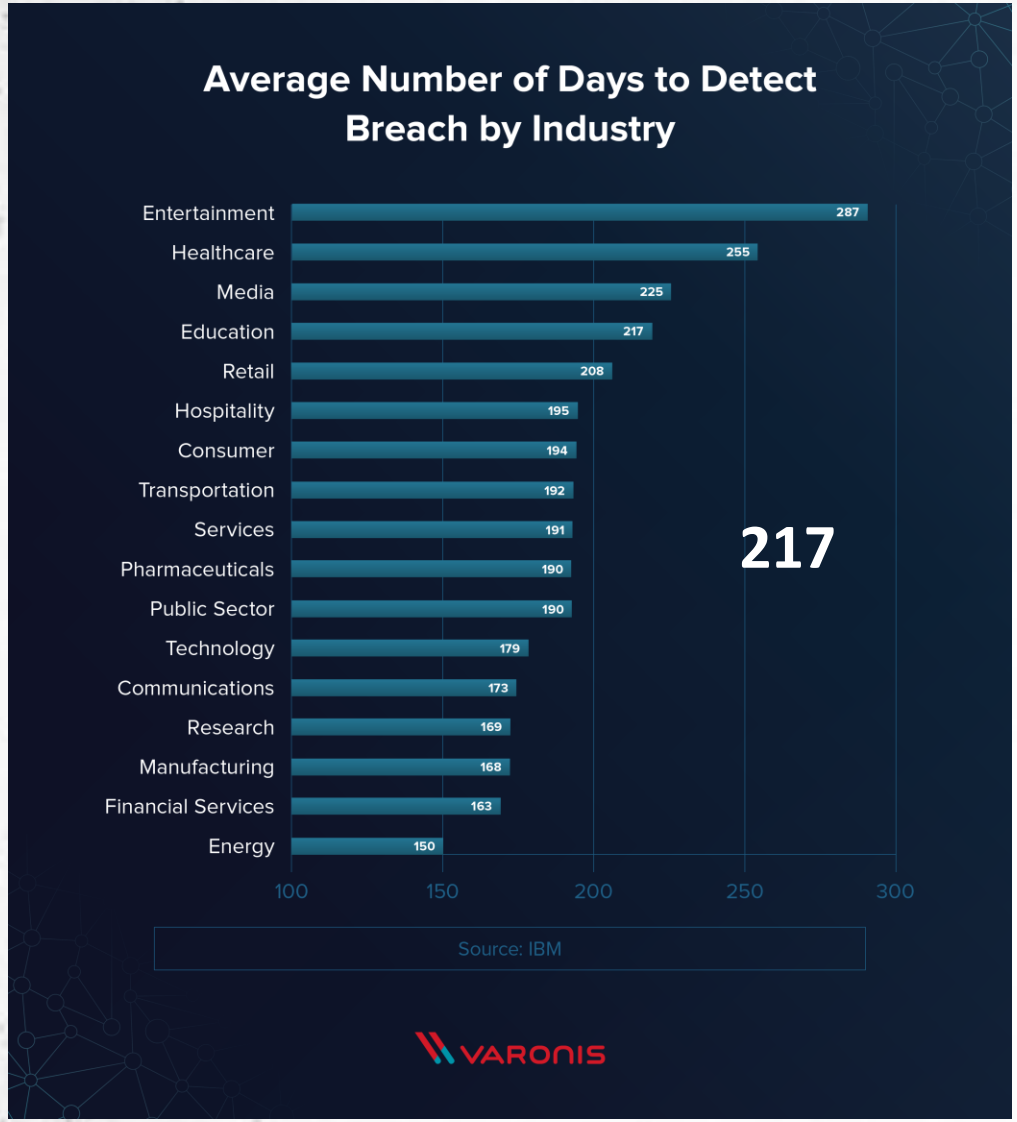
Detekcia

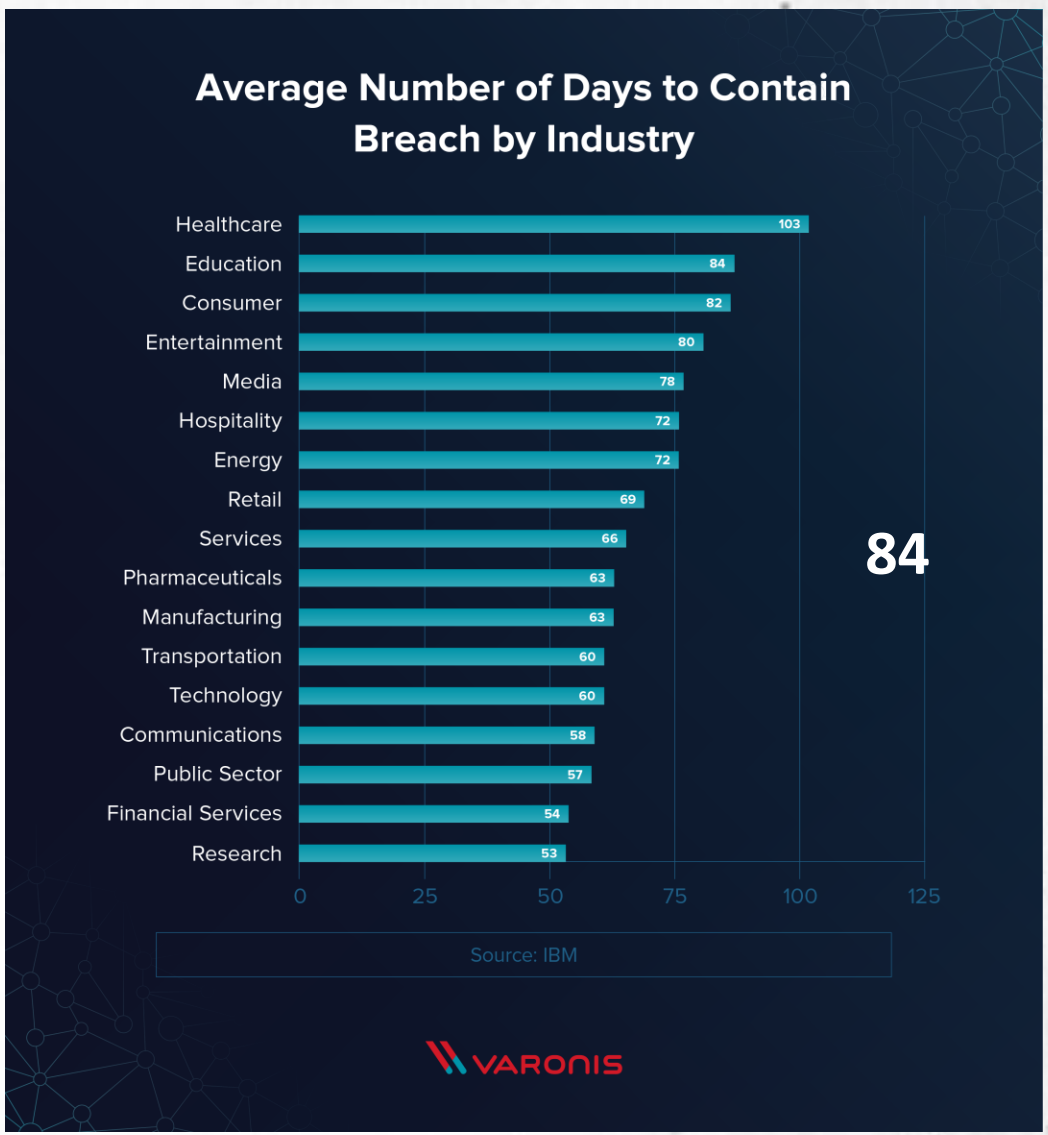
Odpoveď

Proaktívne činnosti

Reaktívne činnosti

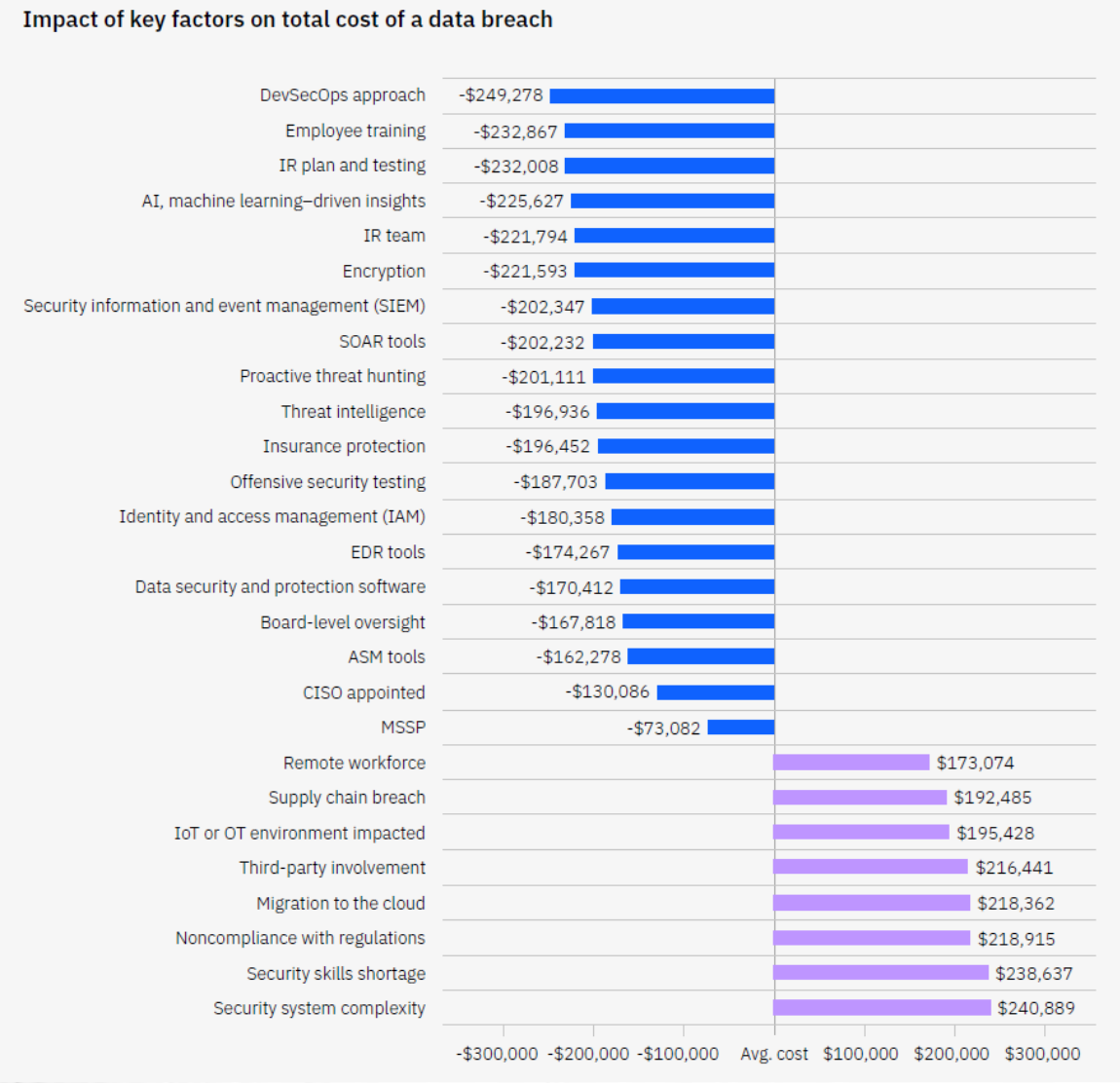
Kontinuita činností (IV.)





Zdroj: https://www.varonis.com/blog/data-breach-response-times/

Kontinuita činností (V.)

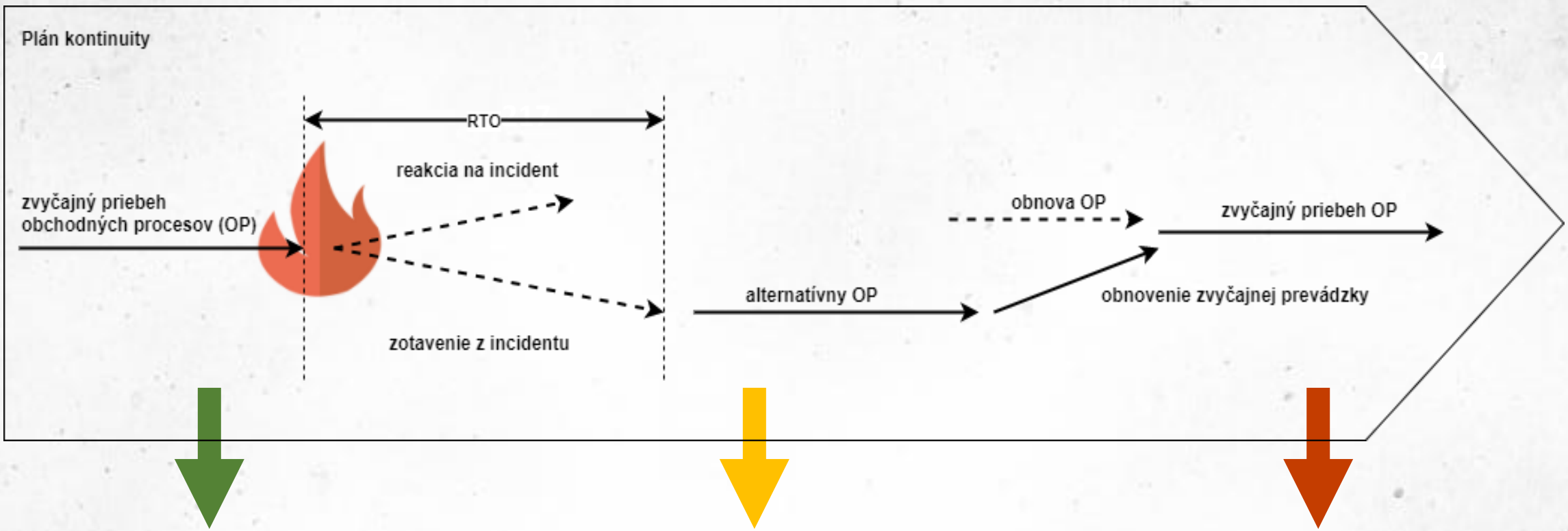


Zdroj: IBM Security - Cost of a Data Breach Report 2023

Faktory:

- Vzdelávanie zamestnancov
- Plány na riešenie incidentov a ich testovanie
- Tím na riešenie incidentov
- Šifrovanie
- Použitie monitorovanie
- ..

Kontinuita činností (VI.)



Reakcia na incident

(IR)

Kontinuita činností

(BC)

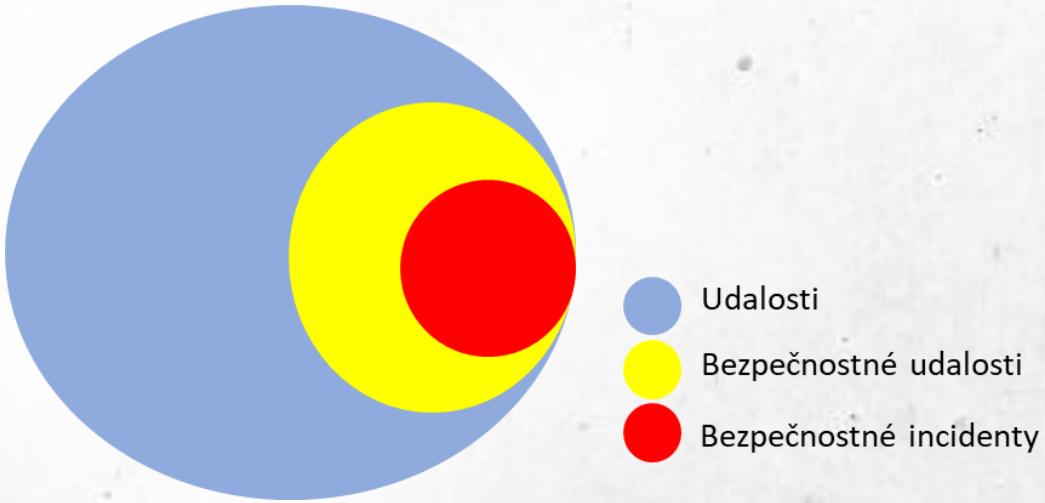
Obnova činností

(BR)

Zdroj: IBM Security - Cost of a Data Breach Report 2023

Bezpečnostný incident

- **Udalosť** – akúkoľvek pozorovateľnú udalosť, ku ktorej došlo v určitom časovom bode v systéme alebo sieti, najmä ak je dôležitá
- **Bezpečnostná udalosť** – pozorovateľná udalosť v prostredí informačných a komunikačných technológií, ktorá je relevantná pre bezpečnosť
- **Bezpečnostný incident** – porušenie alebo bezprostrednú hrozbu porušenia pravidiel počítačovej bezpečnosti, prijateľných zásad používania alebo štandardných bezpečnostných postupov



Cieľ riešenia bezpečnostného incidentu

Zastaviť útok

Zistiť vektor útoku

Zistiť dopad pre organizáciu

Návrh bezpečnostných opatrení

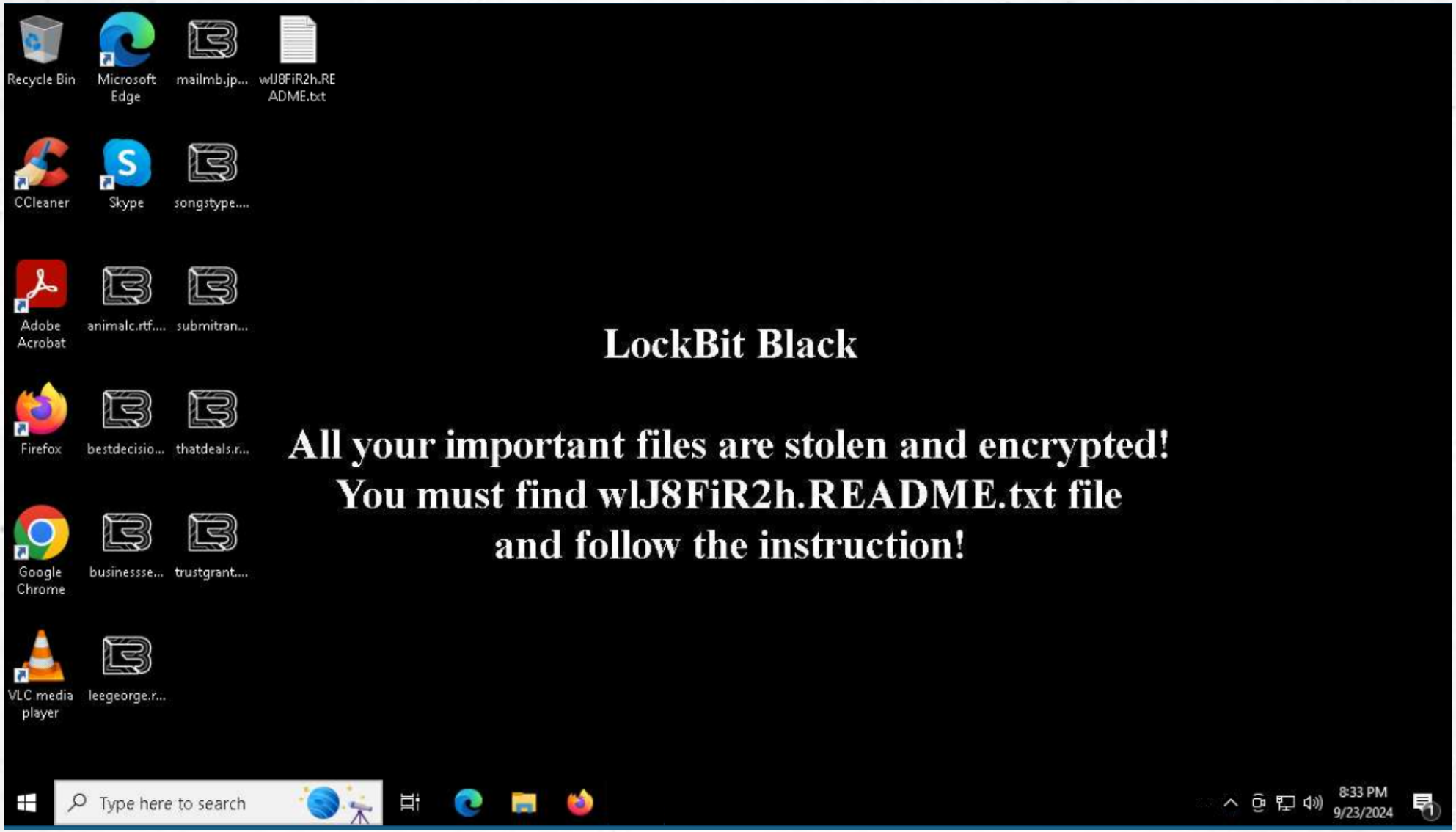
Právny rámec

- Nariadenie Európskeho parlamentu a Rady (EÚ) 2016/679 z 27. apríla 2016 o ochrane fyzických osôb pri spracúvaní osobných údajov a o voľnom pohybe takýchto údajov, ktorým sa zrušuje smernica 95/46/ES (všeobecné nariadenie o ochrane údajov)
- Zákon č. 69/2018 Z. z. o kybernetickej bezpečnosti
- Zákon č. 95/2019 Z. z. o informačných technológiách vo verejnej správe

Zdroj: https://www.a-base.sk/sluzby/bezpecnost/

TEST

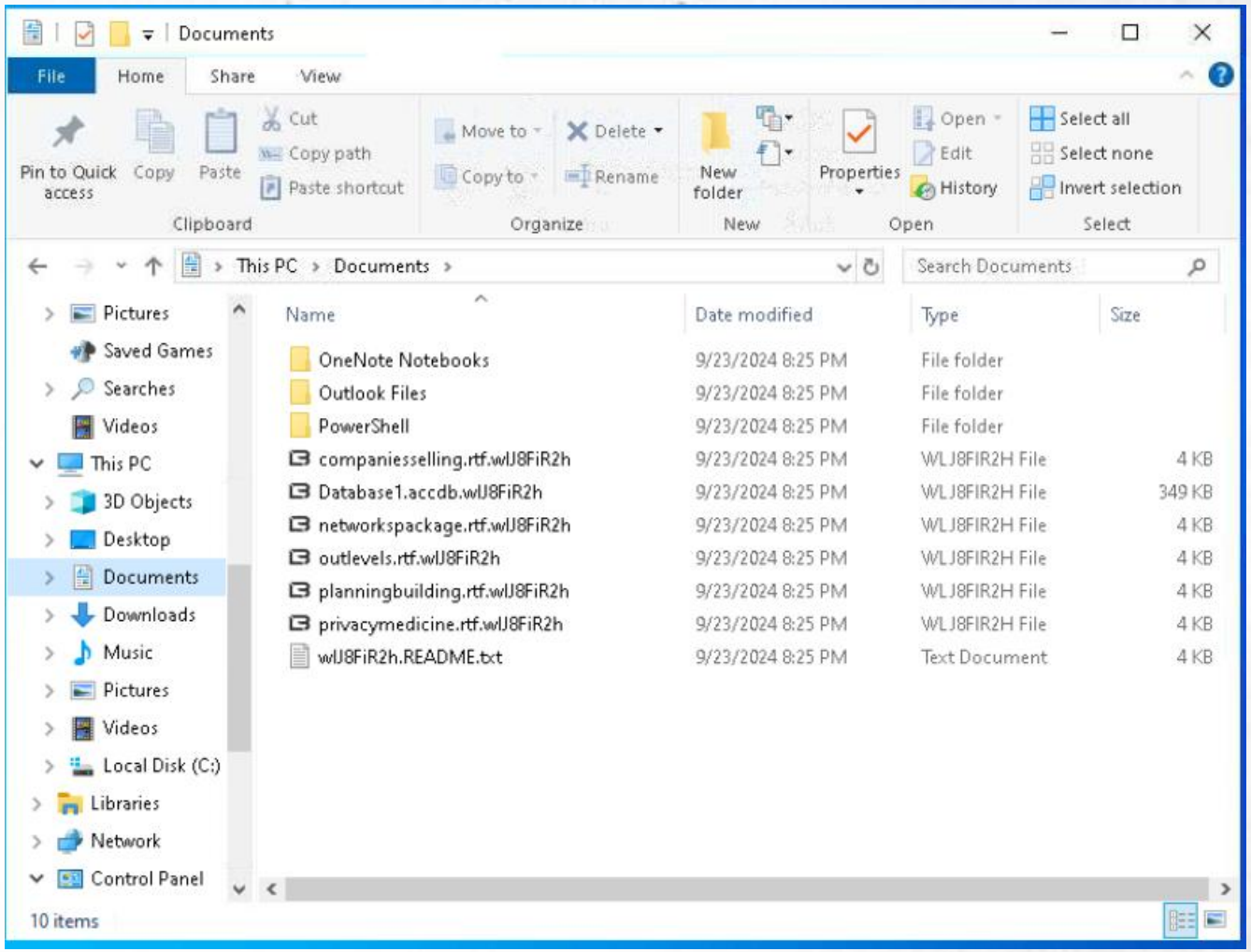
Scenár (I.)



TEST

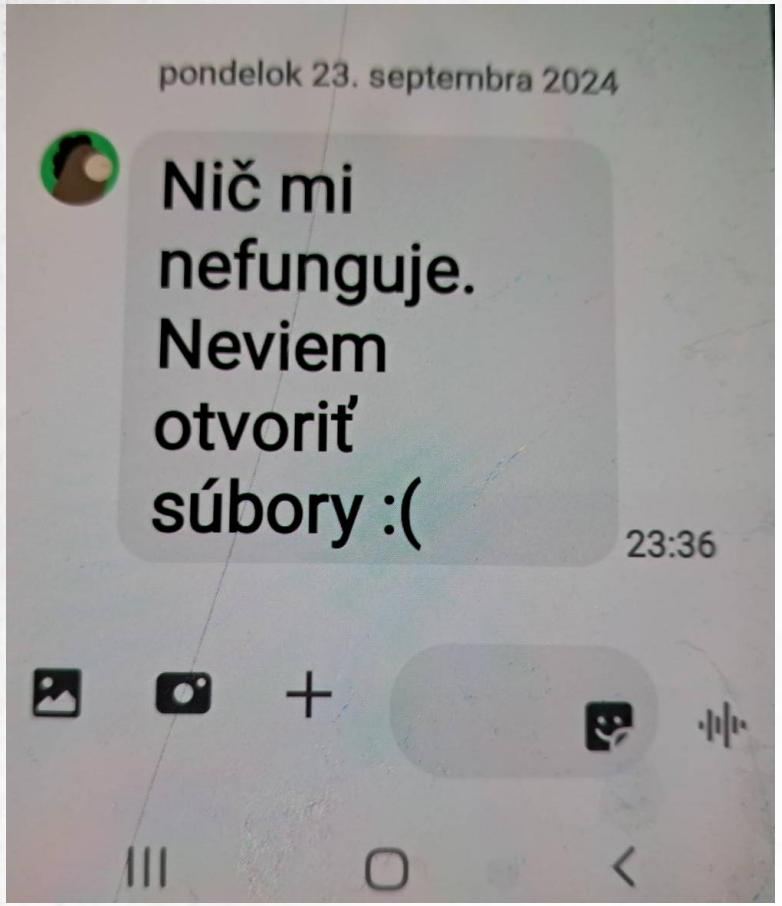
Scenár (II.)

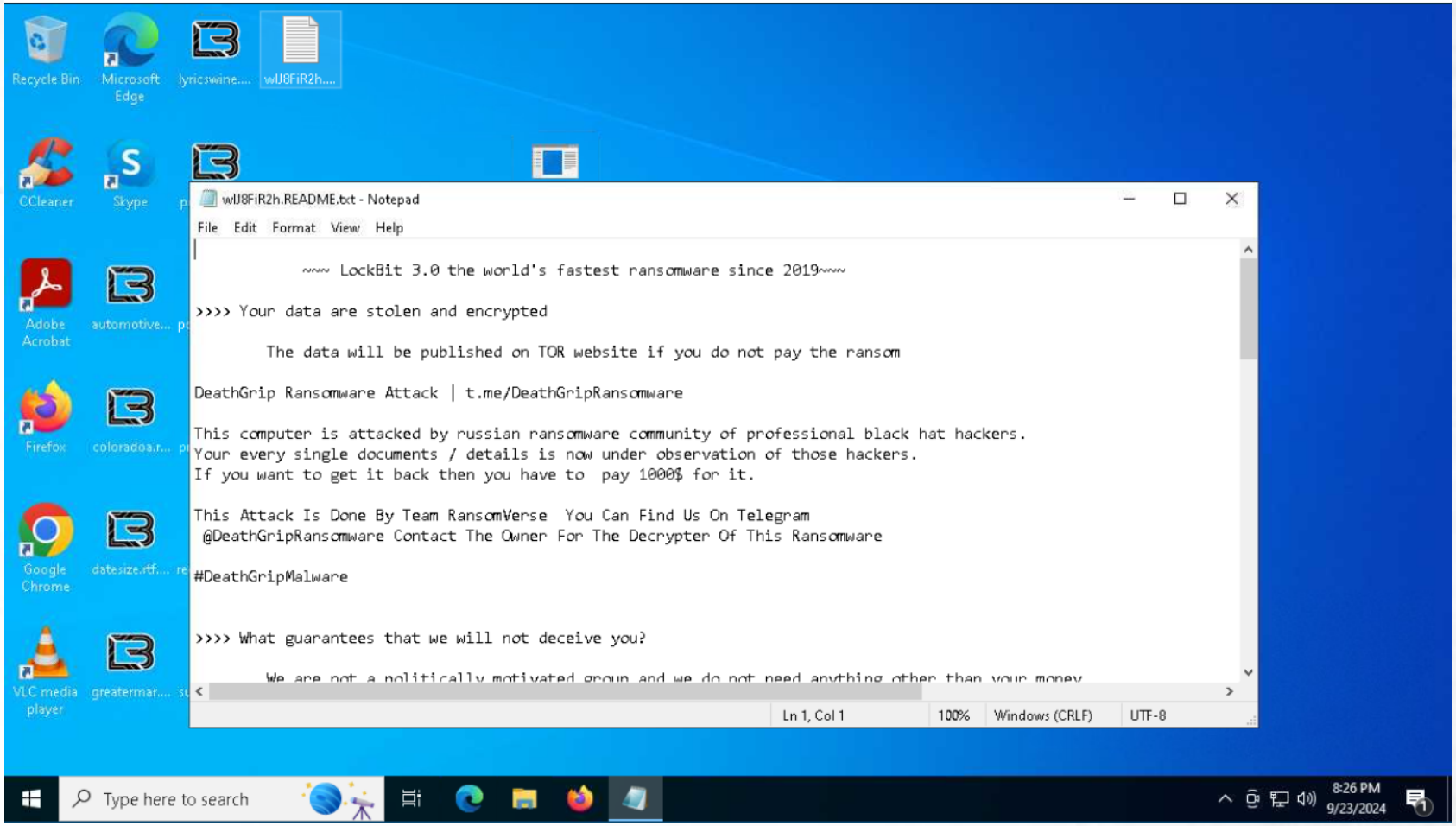
- Nejde otvoriť žiadne súbory
- Dokonca ani na úložisku organizácie
- IT podpora je nedostupná
- Kolegovia volajú/píšu SMS správy



TEST

Scenár (III.)





Aké budú Vaše prvé kroky?

TEST

Scenár (IV.)

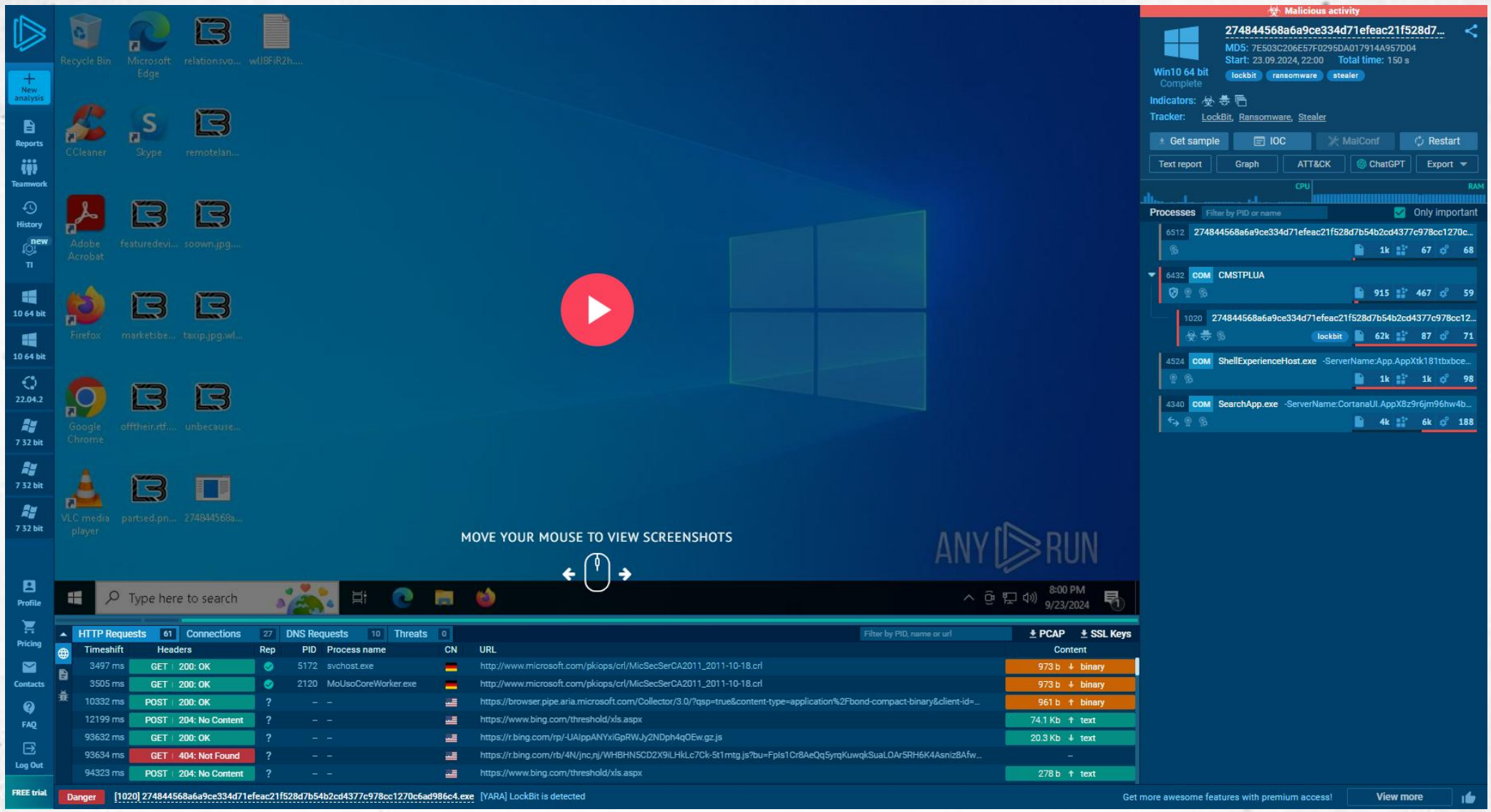
- Ransom note – informácia o výkupnom

> ~~~ LockBit 3.0 the world's fastest and most stable ransomware from 2019~~~
> >>>>> Your data is stolen and encrypted.
> If you don't pay the ransom, the data will be published on our TOR darknet sites. Keep in mind that once your data appears on our leak site, it could be bought by your competitors at any second, so don't hesitate for a long time. The sooner you pay the ransom, the sooner your company will be safe.
> Tor Browser Links:
> -
> Links for normal browser:
> -
> >>>>> What guarantee is there that we won't cheat you?
> We are the oldest ransomware affiliate program on the planet, nothing is more important than our reputation. We are not a politically motivated group and we want nothing more than money. If you pay, we will provide you with decryption software and destroy the stolen data. After you pay the ransom, you will quickly make even more money. Treat this situation simply as a paid training for your system administrators, because it is due to your corporate network not being properly configured that we were able to attack you. Our pentest services should be paid just like you pay the salaries of your system administrators. Get over it and pay for it. If we don't give you a decryptor or delete your data after you pay, no one will pay us in the future. You can get more information about us on Ilon Musk's Twitter hxxps://twitter.com/hashtag/lockbit?f=live
>
> >>>>> You need to contact us and decrypt one file for free on TOR darknet sites with your personal ID
> Download and install Tor Browser hxxps://www.torproject.org/
> Write to the chat room and wait for an answer, we'll guarantee a response from you. If you need a unique ID for correspondence with us that no one will know about, tell it in the chat, we will generate a secret chat for you and give you his ID via private one-time memos service, no one can find out this ID but you. Sometimes you will have to wait some time for our reply, this is because we have a lot of work and we attack hundreds of companies around the world.
> Tor Browser Links for chat:

Tor Browser Links for chat:
-
>>
>>>>> Your personal ID: - <<<<<
>>
>>>>> Warning! Do not delete or modify encrypted files, it will lead to problems with decryption of files!
>>>>> Don't go to the police or the FBI for help and don't tell anyone that we attacked you.
They won't help and will only make things worse for you. In 3 years not a single member of our group has been caught by the police, we are top notch hackers and we never leave a trail of crime. The police will try to prohibit you from paying the ransom in any way. The first thing they will tell you is that there is no guarantee to decrypt your files and remove stolen files, this is not true, we can do a test decryption before paying and your data will be guaranteed to be removed because it is a matter of our reputation, we make hundreds of millions of dollars and are not going to lose our revenue because of your files. It is very beneficial for the police and FBI to let everyone on the planet know about your data leak because then your state will get the fines budgeted for you due to GDPR and other similar laws. The fines will be used to fund the police and the FBI, they will eat more sweet coffee donuts and get fatter and fatter. The police and the FBI don't care what losses you suffer as a result of our attack, and we will help you get rid of all your problems for a modest sum of money. Along with this you should know that it is not necessarily your company that has to pay the ransom and not necessarily from your bank account, it can be done by an unidentified person, such as any philanthropist who loves your company, for example, Elon Musk, so the police will not do anything to you if someone pays the ransom for you. If you're worried that someone will trace your bank transfers, you can easily buy cryptocurrency for cash, thus leaving no digital trail that someone from your company paid our ransom. The police and FBI will not be able to stop lawsuits from your customers for leaking personal and private information. The police and FBI will not protect you from repeated attacks. Paying the ransom to us is much cheaper and more profitable than paying fines and legal fees.
>>>>> What are the dangers of leaking your company's data.
First of all, you will receive fines from the government such as the GDRP and many others, you can be sued by customers of your firm for leaking information that was confidential. Your leaked data will be used by all the hackers on the planet for various unpleasant things. For example, social engineering, your employees' personal data can be used to re-infiltrate your company. Bank details and passports can be used to create bank accounts and online wallets through which criminal money will be laundered. On another vacation trip, you will have to explain to the FBI where you got millions of dollars worth of stolen cryptocurrency transferred through your accounts on cryptocurrency exchanges. Your personal information could be used to make loans or buy appliances. You would later have to prove in court that it wasn't you who took out the loan and pay off someone else's loan. Your competitors may use the stolen information to steal technology or to improve their processes, your working methods, suppliers, investors, sponsors, employees, it will all be in the public domain. You

Ako postupovať ďalej?

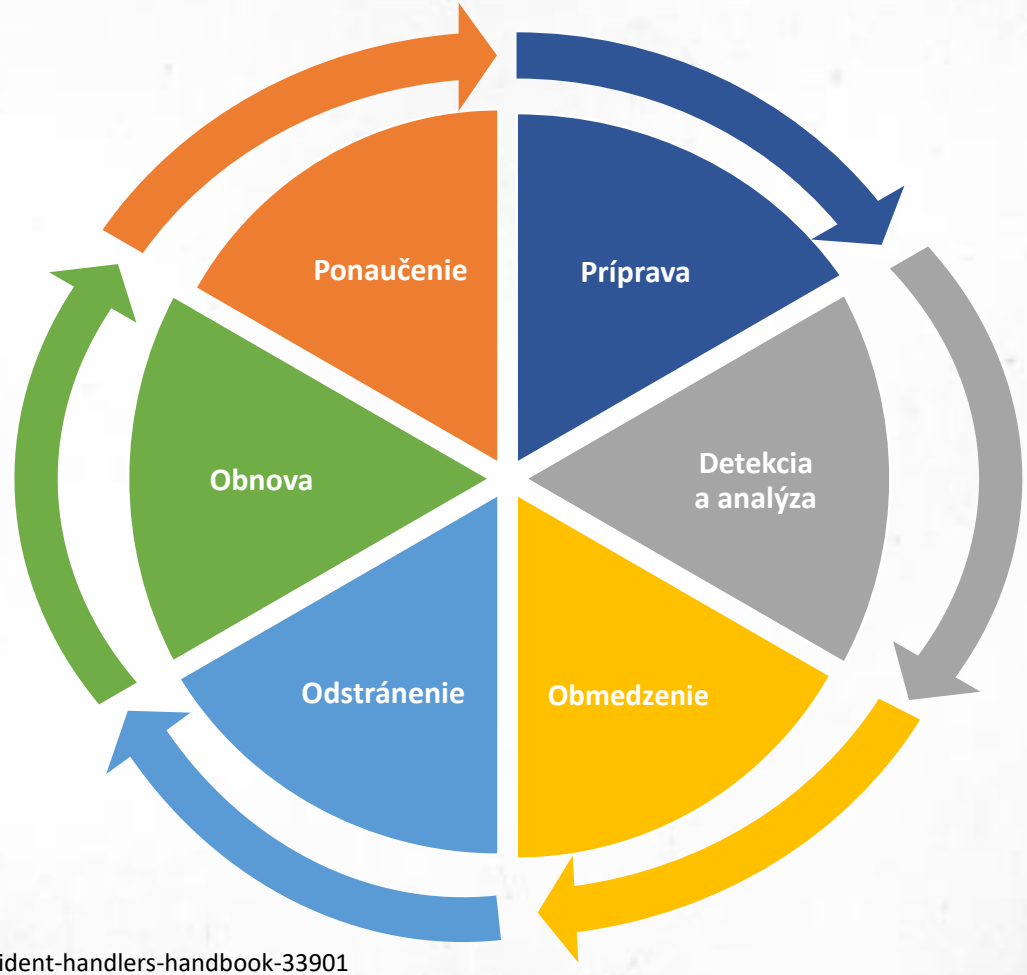
Ukážka ransomvér útoku



Zdroj: https://app.any.run/tasks/7c048de1-ccdc-47df-9f0f-985cf31dea76

Postup riešenia bezpečnostného incidentu

- Fázy riešenia bezpečnostných incidentov podľa **SANS**



Zdroj: https://www.sans.org/reading-room/whitepapers/incident/incident-handlers-handbook-33901

Identifikácia bezpečnostných incidentov

- Incidentom sa vždy nedá zabrániť, musia sa však vždy identifikovať
- **Externé zdroje**
  - Iné organizácie – hlásenia (SK-CERT,...)
  - Automatizované systémy (napr. have I been pwned?)
- **Interné zdroje**
  - Nahlasovanie cez kontaktné miesto (email/telefón)
  - Monitorovanie (SIEM)
  - Vlastná dohľadávacia činnosť
- ***Ako identifikujete bezpečnostné incidenty?***

Nahlásenie incidentu

Ak chcete nahlásiť incident, zavolajte na niektoré z týchto telefónnych čísel alebo nám pošlite email. Všetky potrebné detaily si od Vás počas rozhovoru vypýtame.

+421 55 234 1111

incident@upjs.sk

Pracovné hodiny: 8:00-16:00

Všeobecný email

csirt@upjs.sk

Facebook

CSIRT-UPJS

Adresa

CSIRT
Univerzita Pavla Jozefa Šafárika
Šrobárova 2
041 80 Košice

PGP kľúč

```
User ID: CSIRT team UPJS <csirt@upjs.sk>
Key ID: 0x0C62E396</csirt@upjs.sk>
Exp: n/a
Fingerprint: BBD5 D706 CBA1 FD9D 3A3B 0B9E 2AF6 8D10 0C62 E396
```

Zdroj: https://csirt.upjs.sk/#/kontakt

Analýza bezpečnostných incidentov

- Overiť si udalosť
- Bezpečnostný incident vs. technický incident
- Určenie typu bezpečnostného incidentu
  - Zdieľanie informácií
  - Spustenie špecifického postupu
- Predbežné určenie rozsahu
  - **určenie rozsahu** - identifikácia systémov, ľudí a informačných aktív, ktoré sú súčasťou udalosti.
  - **podozrivé udalosti** – nové účty, modifikácia súborov, zmeny vo výkone a pod.
- ***Máte IT oddelenie? Špecifický postup?***

Taxonómia bezpečnostných incidentov (I.)

- eCSIRT.net mkIV.
- CIRCL.LU taxonómia,
- Spoločná taxonómia pre orgány činné v trestnom konaní a jednotky CSIRT (Common Taxonomy for LE and CSIRTs).

REFERENCE TAXONOMY INCIDENT CLASSIFICATION (1ST COLUMN)	INCIDENT EXAMPLES (2ND COLUMN)
Malicious Code	Virus
	Worm
	Trojan
	Spyware
	Dialler
	Rootkit

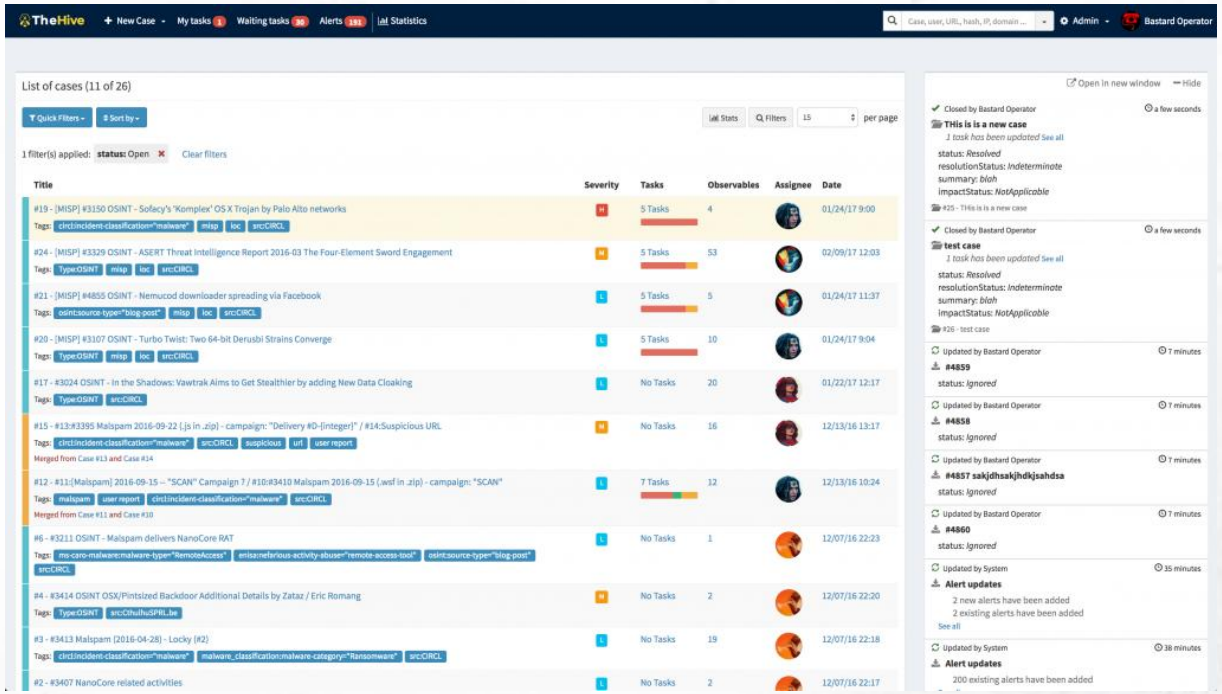
INCIDENT TYPE (2ND COLUMN)	COMMON TAXONOMY FOR LEA AND CSIRT INCIDENT CLASSIFICATION (1ST COLUMN)
Infection	Malware
Distribution	
C&C	
Undetermined	
Malicious Connection	

Zdroj: https://www.trusted-introducer.org/Incident-Classification-Taxonomy.pdf

Evidencia bezpečnostného incidentu

- **Evidencia bezpečnostných incidentov**
  - Tiketovací systém / Interná evidencia (emailové správy)
  - Zaznamenajte si postup + dôležité údaje

Ako by ste evidovali bezpečnostný incident?



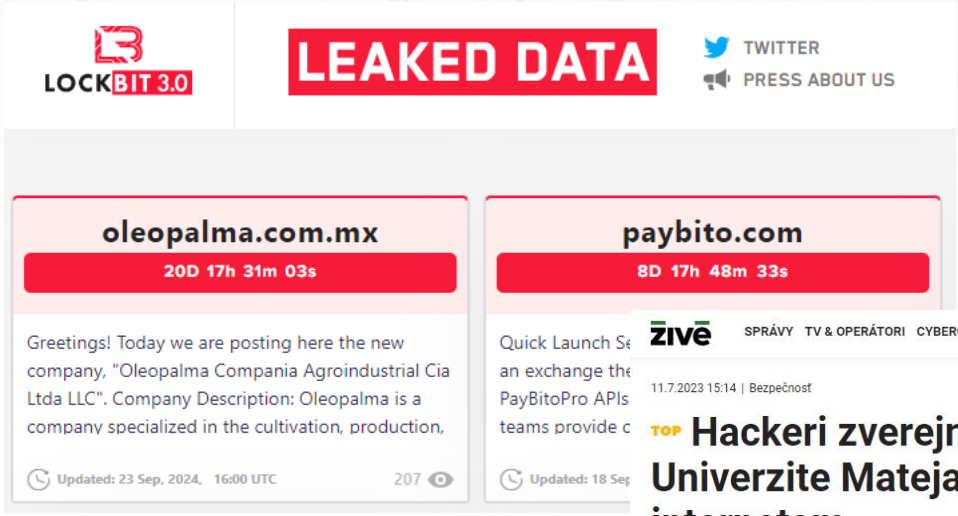
Zdroj: https://strangebee.com/thehive/

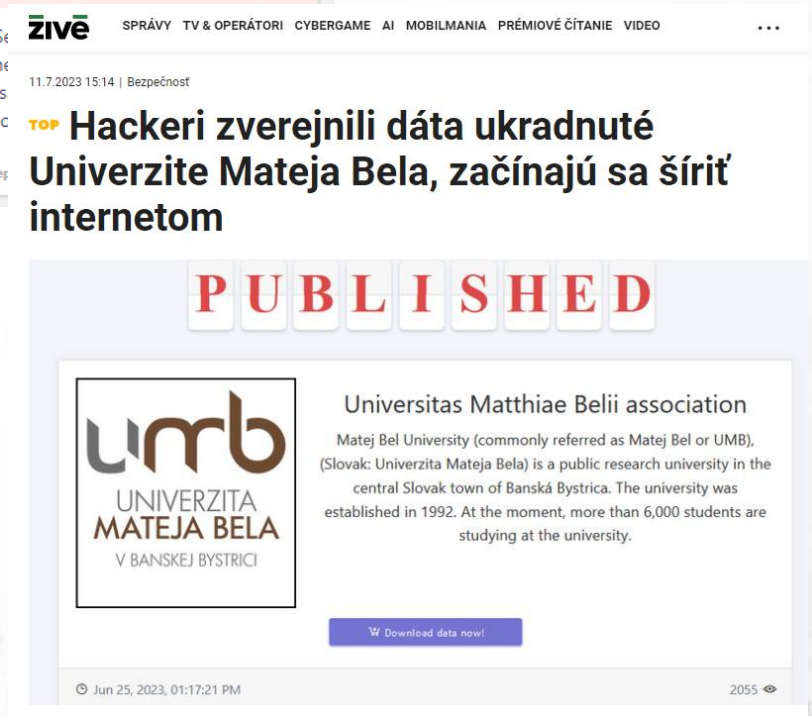
Komunikácia bezpečnostného incidentu (I.)

Zdroj: https://docs.opencti.io/latest/administration/segregation/

Komunikácia bezpečnostného incidentu (II.)

- Partneri/klienti
- Média
  - Nahlásiť
  - Zamestnanci / útočník
- OČTK
- Povinné / dobrovoľné hlásenia
  - Úrad na ochranu osobných údajov
  - NBÚ, Telekomunikačný úrad
- ***Komu by ste hlásili/komunikovali bezpečnostný incident a aký spôsobom?***





Zdroj: https://zive.aktuality.sk/clanok/cfRr3Xq/hackeri-zverejnili-data-ukradnute-univerzite-mateja-bela-zacinaju-sa-sirit-internetom/

Komunikácia bezpečnostného incidentu (III.)

Bezpečnostný pohľad

- Bezpečnostný incident
- CSIRT / Dohľadový orgán
- Zastaviť incident, zistiť dopad incidentu, zamedziť rovnakému incidentu

Trestnoprávny pohľad

- Skutok
- Orgány činné v trestnom konaní
- Nájsť páchateľa

Pohľad ochrany osobných údajov

- Bezpečnostný incident
- ÚOOÚ
- Identifikovať dopad na OOÚ a urobiť opatrenia

Komunikácia bezpečnostného incidentu (IV.)

Čl. 33 GDPR

Ktoré incidenty je potrebné oznámiť podľa GDPR?

- Porušenie ochrany osobných údajov
- Porušenie bezpečnosti

Kto musí oznamovať?

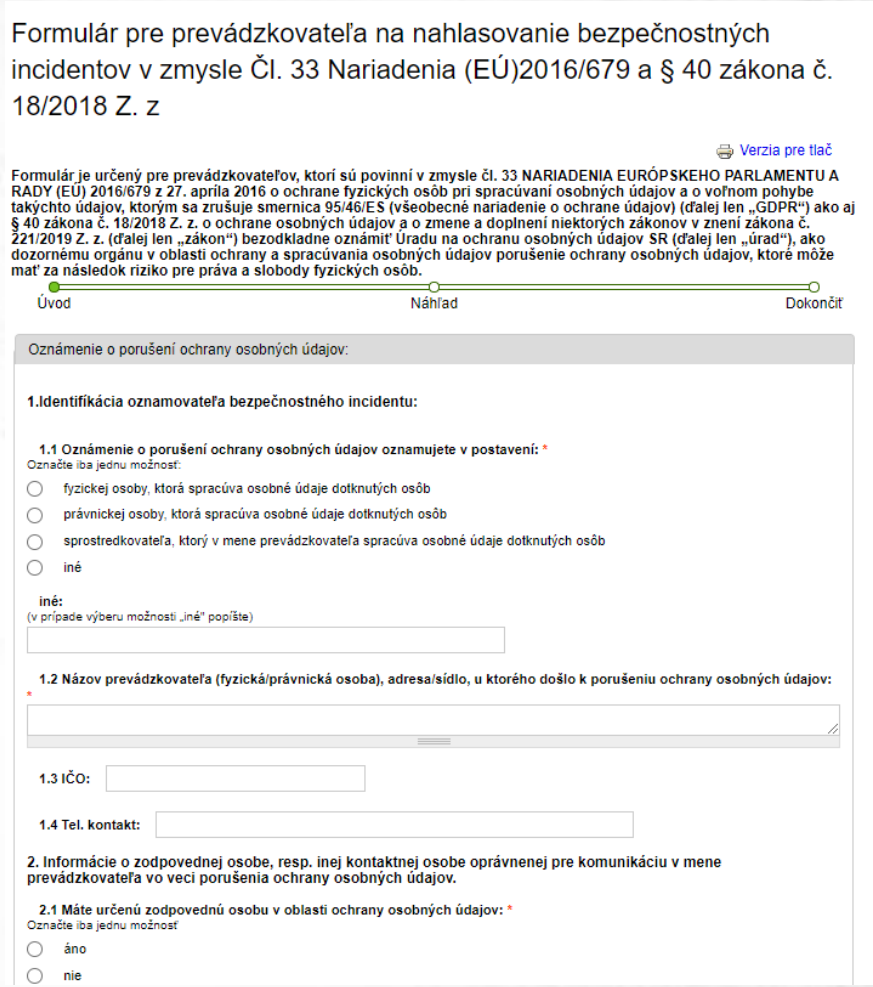
- Každý prevádzkovateľ a sprostredkovateľ

Komu je potrebné incident oznámiť?

- Úradu na ochranu osobných údajov
- Dotknutým osobám (niektoré prípady)

Do kedy je potrebné incident oznámiť?

- **Bez zbytočného odkladu**, resp. **do 72 hodín**



Formulár pre prevádzkovateľa na nahlasovanie bezpečnostných incidentov v zmysle Čl. 33 Nariadenia (EÚ)2016/679 a § 40 zákona č. 18/2018 Z. z

Verzia pre tlač

Formulár je určený pre prevádzkovateľov, ktorí sú povinní v zmysle čl. 33 NARIADENIA EURÓPSKEHO PARLAMENTU A RADY (EÚ) 2016/679 z 27. apríla 2016 o ochrane fyzických osôb pri spracúvaní osobných údajov a o voľnom pohybe takýchto údajov, ktorým sa zrušuje smernica 95/46/ES (všeobecné nariadenie o ochrane údajov) (ďalej len „GDPR") ako aj § 40 zákona č. 18/2018 Z. z. o ochrane osobných údajov a o zmene a doplnení niektorých zákonov v znení zákona č. 221/2019 Z. z. (ďalej len „zákon") bezodkladne oznámiť Úradu na ochranu osobných údajov SR (ďalej len „úrad"), ako dozornému orgánu v oblasti ochrany a spracúvania osobných údajov porušenie ochrany osobných údajov, ktoré môže mať za následok riziko pre práva a slobody fyzických osôb.

Úvod — Náhľad — Dokončiť

Oznámenie o porušení ochrany osobných údajov:

1.Identifikácia oznamovateľa bezpečnostného incidentu:

1.1 Oznámenie o porušení ochrany osobných údajov oznamujete v postavení: *
Označte iba jednu možnosť:
- fyzickej osoby, ktorá spracúva osobné údaje dotknutých osôb
- právnickej osoby, ktorá spracúva osobné údaje dotknutých osôb
- sprostredkovateľa, ktorý v mene prevádzkovateľa spracúva osobné údaje dotknutých osôb
- iné

iné:
(v prípade výberu možnosti „iné" popíšte)

1.2 Názov prevádzkovateľa (fyzická/právnická osoba), adresa/sídlo, u ktorého došlo k porušeniu ochrany osobných údajov: *

1.3 IČO:

1.4 Tel. kontakt:

2. Informácie o zodpovednej osobe, resp. inej kontaktnej osobe oprávnenej pre komunikáciu v mene prevádzkovateľa vo veci porušenia ochrany osobných údajov.

2.1 Máte určenú zodpovednú osobu v oblasti ochrany osobných údajov: *
Označte iba jednu možnosť
- áno
- nie

https://dataprotection.gov.sk/sk/prevadzkovatelia/oznamenie-poruseni-ochrany-osobnych-udajov/

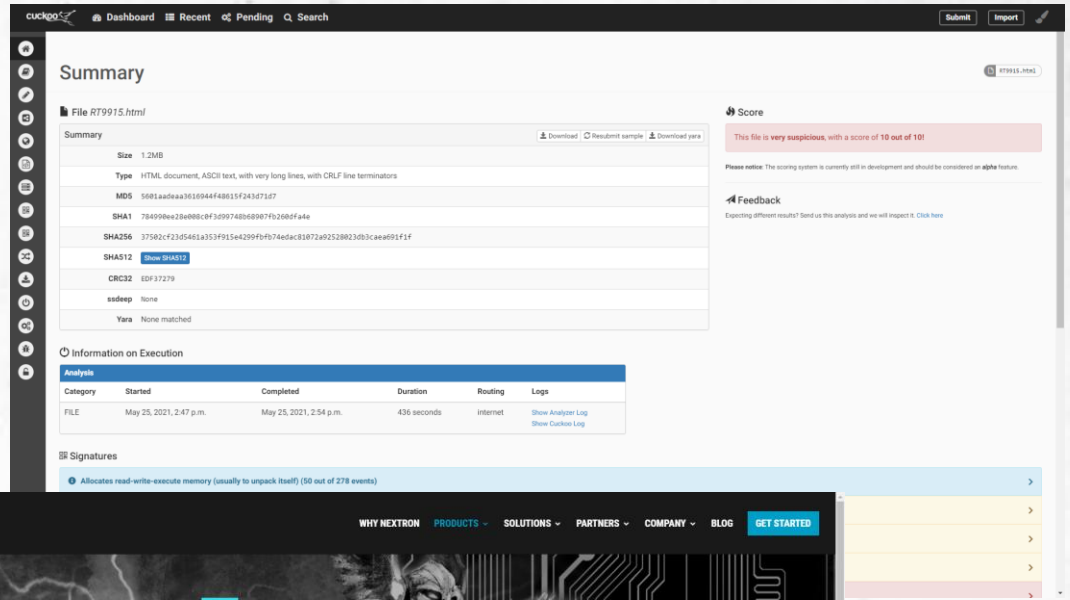
Zastavenie/Obmedzenie bezpečnostného incidentu

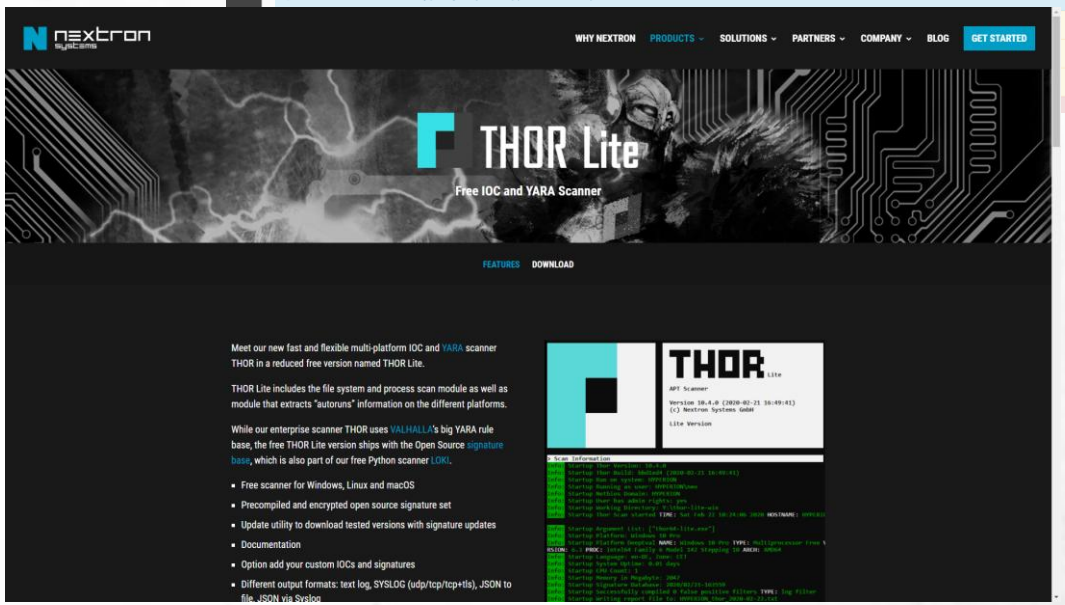
- **Blokovanie ďalšieho prístupu** alebo poškodenia systémov
  - Vypnutie systému, odpojenie od siete, zmena pravidiel,
  - Zvýšenie úrovne monitorovania
  - Malvér -> **izolácia** kompromitivaných systémov
  - Phishing -> **deaktivácia** odkazu

- ***Čo by ste robili v prípade ransomvér útoku?***

Analýza bezpečnostného incidentu

- **Zhromažďovanie digitálnych stôp** – zaisťovanie
- Zhromaždenie podrobností o vektore útoku a o krokoch podniknutých s cieľom umožniť účinné odstránenie
- Výrazne technická časť
- Viacero free/open-source nástroj

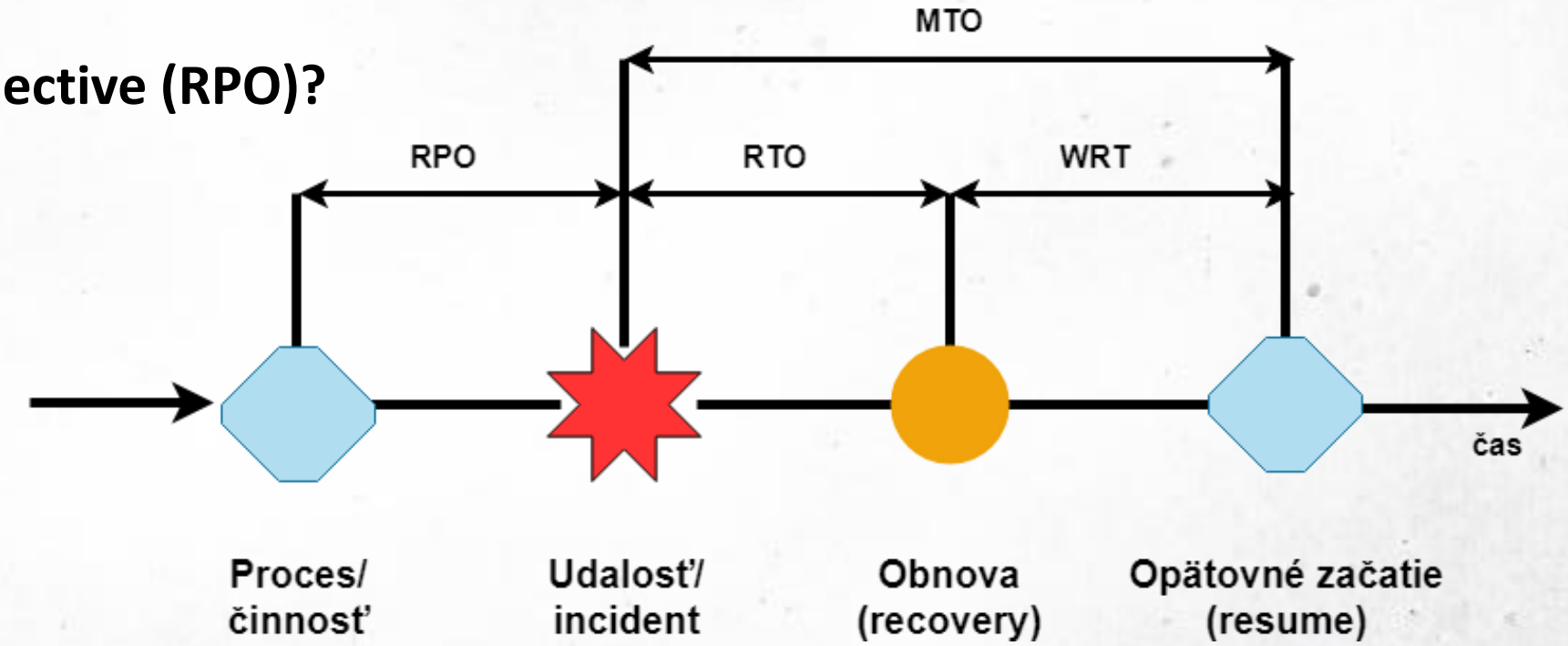




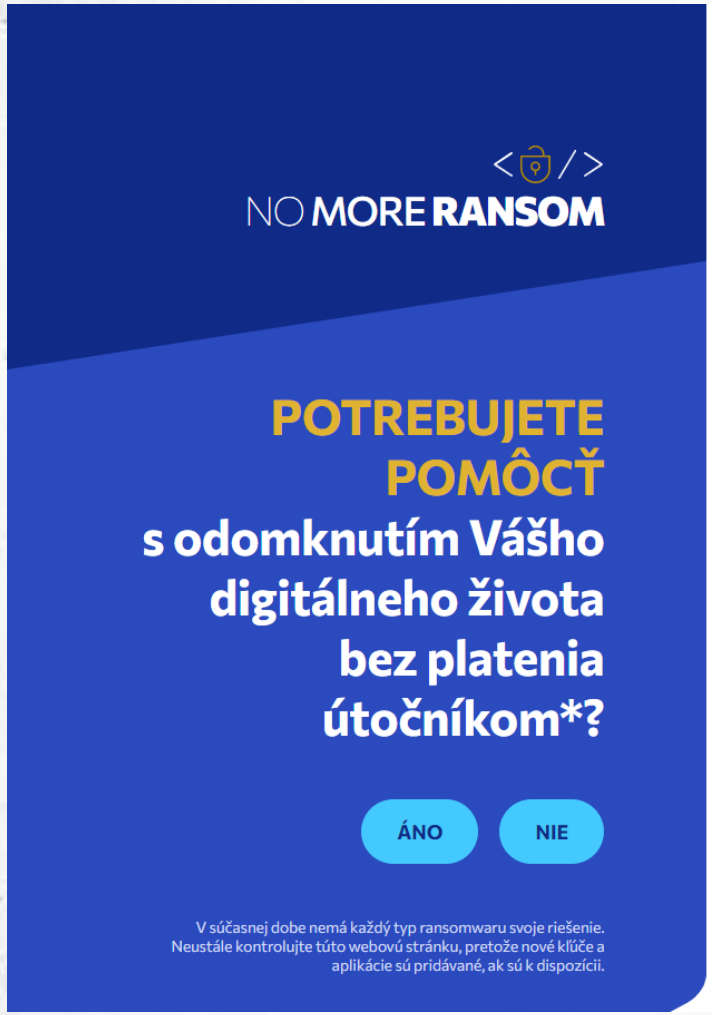
https://cuckoo.cert.ee/analysis/2232081/summary/ https://www.nextron-systems.com/thor-lite/

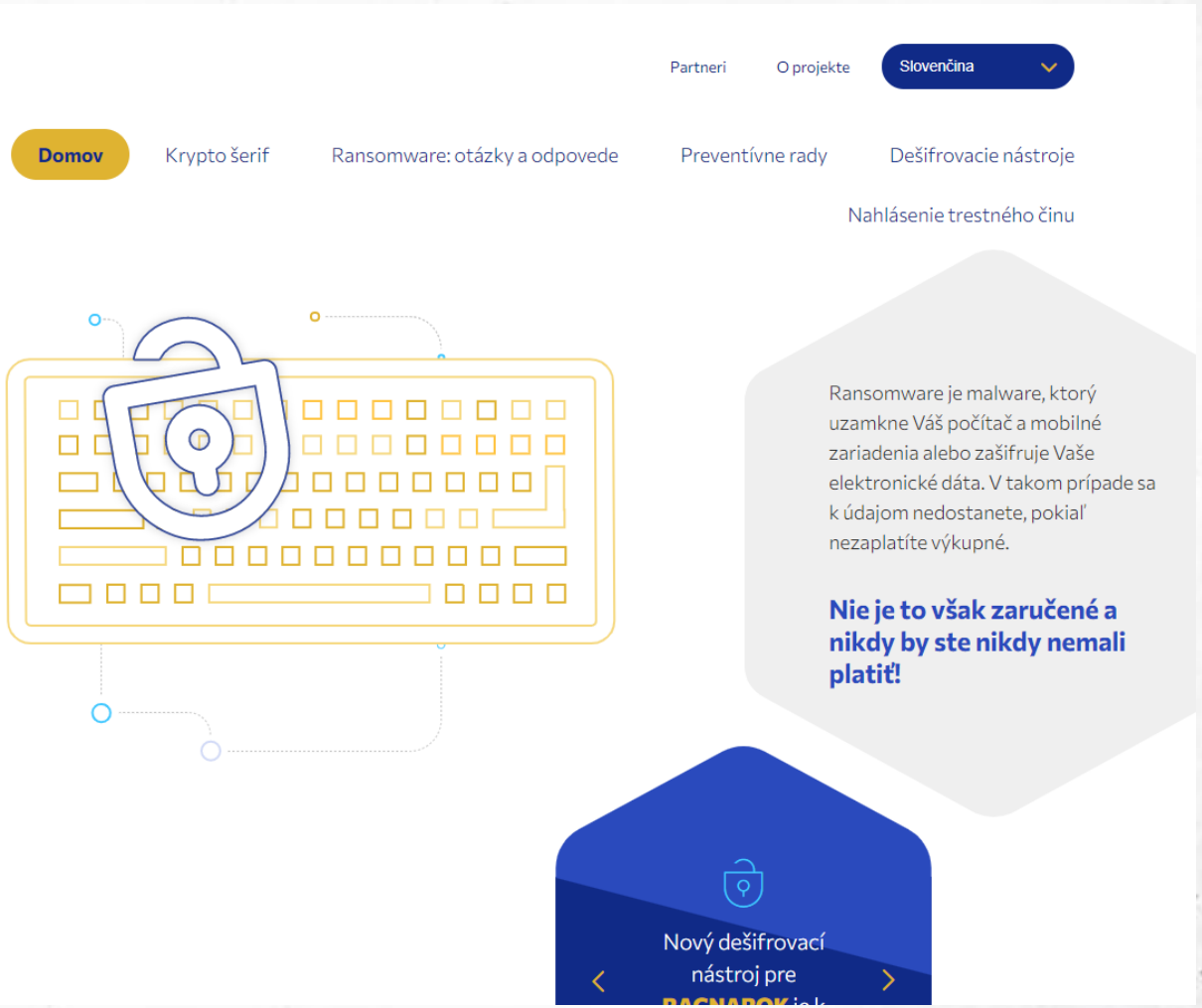
Odstránenie príčiny a obnova dát / systémov (I.)

- Identifikácia bezpečnostných zraniteľností
- Zálohy / zálohovacie systémy – 1 z cieľov útočníkov
- **Recovery point objective (RPO)?**



Odstránenie príčiny a obnova dát / systémov (II.)





https://www.nomoreransom.org/sk/index.html

Uzavretie a príprava na bezpečnostný incident

- **Uzavretie bezpečnostného incidentu**
  - Aký by bol dopad u Vás?
  - Aké systémy boli zasiahnuté?
  - Bezpečnostné opatrenia?
- **Lessons learned**
  - Ako to robiť inak?
  - **Štruktúra** siete, **inventarizácia** zariadení
  - **Prístupy** k zariadeniam (najmä sieťovým prvkom)
  - **Postupy**
    - Aké kroky vykonať
    - Koho informovať
  - **Nástroje**
    - Množstvo open-source nástrojov

Zdroj: https://www.bydfi.com/blog/topic/blockchain/history-of-cryptography/

Kryptológia

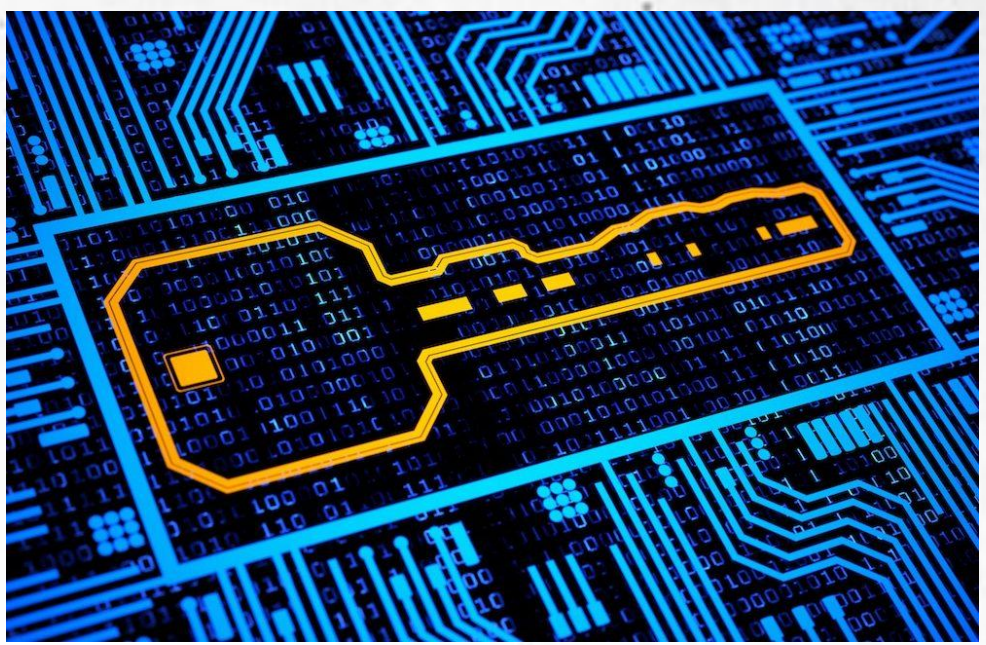
- Gréc. kryptos = ukrytý + logos = slovo
- Veda o utajovaní správ
- Delenie:
  - **Kryptografia** – návrh systémov na zabezpečenie údajov
    - Algoritmus
    - Časová zložitosť
    - Bezpečnosť
  - **Kryptoanalýza** – návrh možnosti útokov na kryptografické systémy

Kryptológia v minulosti

Zdroj: https://en.wikipedia.org/wiki/Scytale#/media/File:Skytale.png, https://similarpng.com/encryption-key-logo-on-transparent-background-png/#getdownload, https://www.enisa.europa.eu/news/enisa-news/cryptographic-tools-are-important-for-civil-society-and-industry/@@images/09f8915a-84a4-4fee-9753-94aa770f7424.jpeg. https://www.hiclipart.com/free-transparent-background-png-clipart-mmffu/download

Kryptológia v súčasnosti

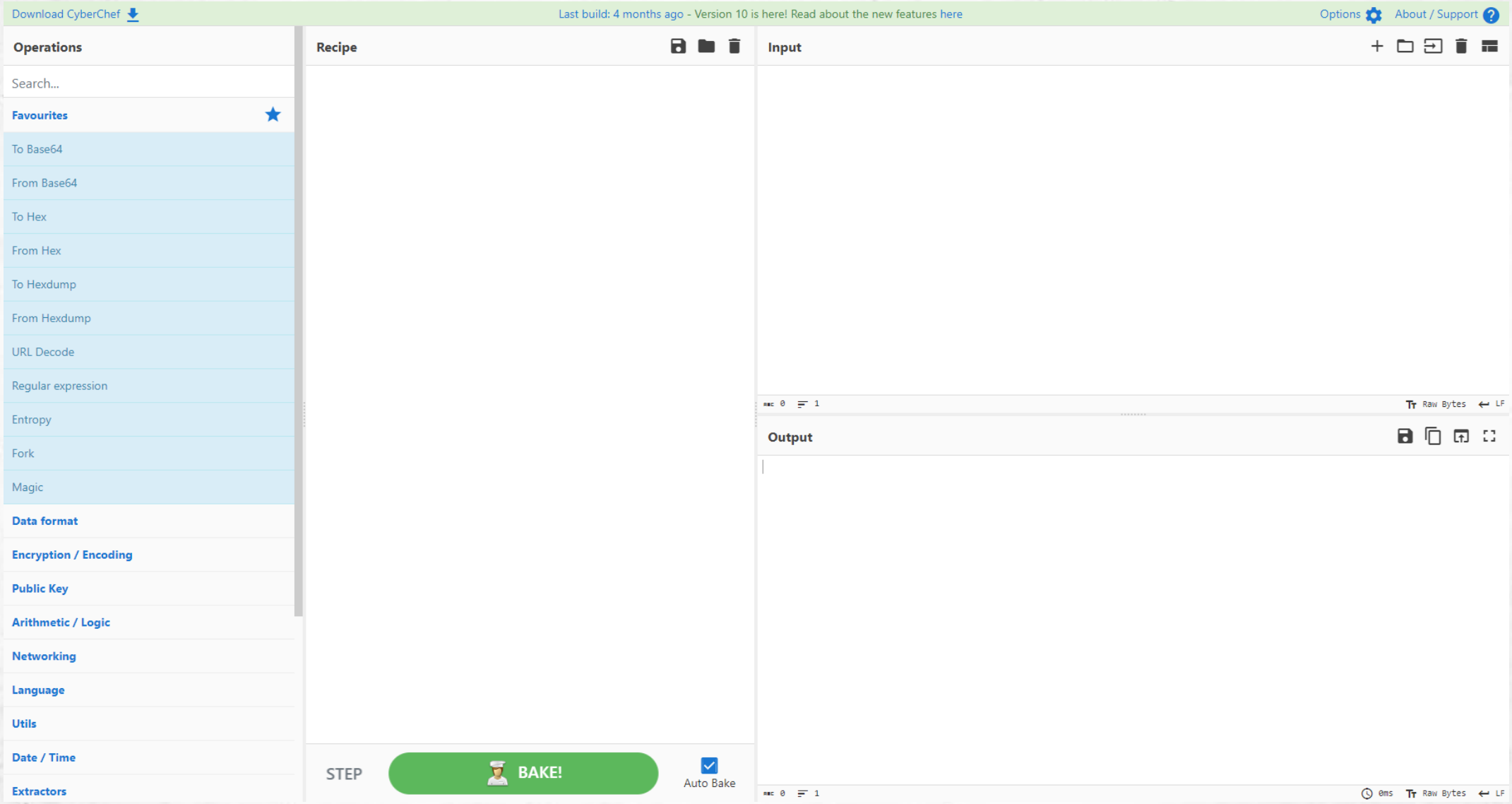
- Utajovanie dokumentov
- Zabezpečenie prehliadania internetových stránok
- Zabezpečenie hesiel
- Zabezpečenie prevodu peňazí – platba kartou
- Anonymizácia podľa právnych predpisov
- ...



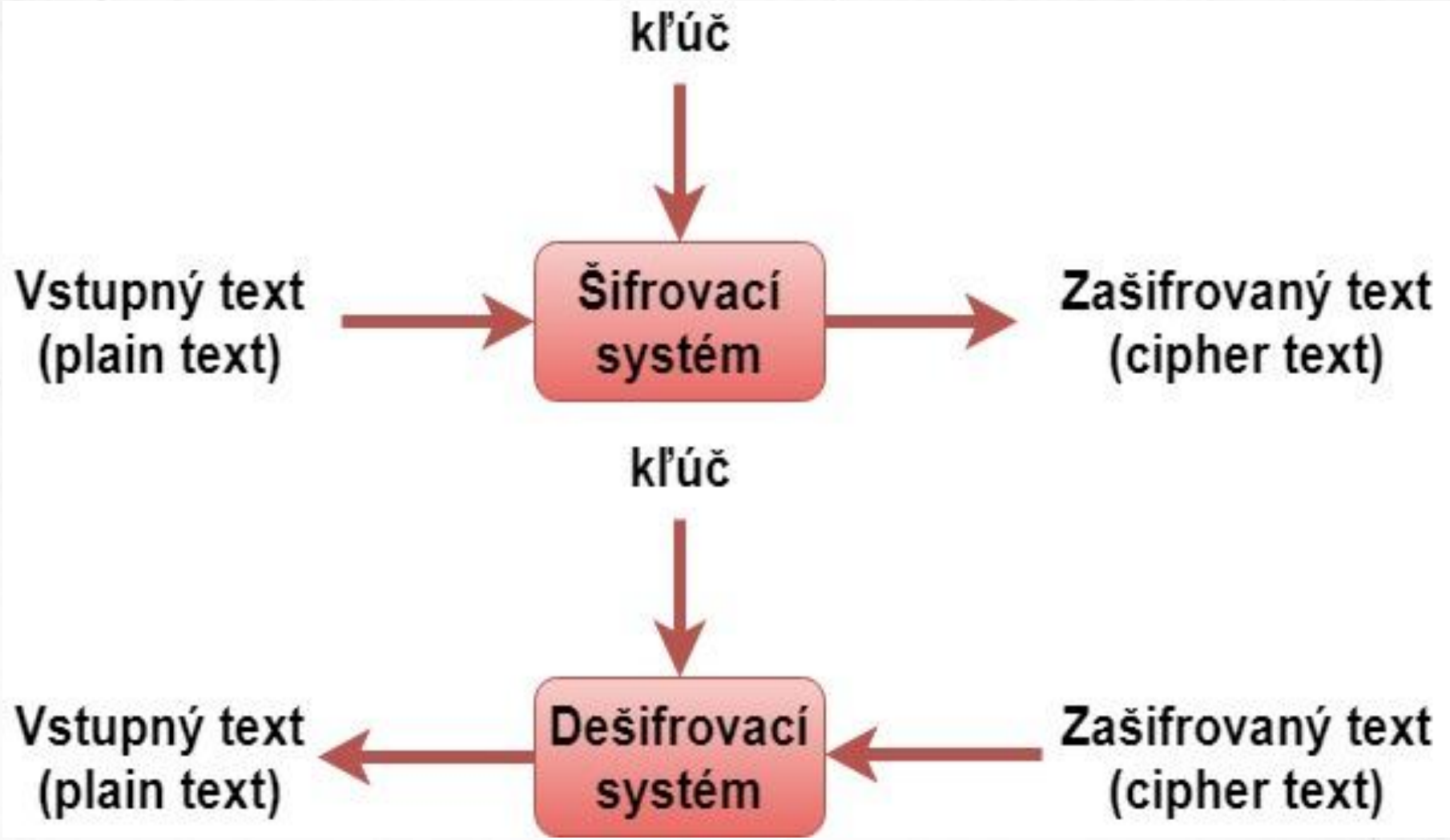
Zdroj: https://medium.com/@prashanthreddyt1234/real-life-applications-of-cryptography-162ddf2e917d, https://arstechnica.com/information-technology/2024/10/the-sad-bizarre-tale-of-hype-fueling-fears-that-modern-cryptography-is-dead/#gsc.tab=0, https://kosicednes.sk/spravy/rezort-vnutra-planuje-vydavat-bezkontaktne-biometricke-obcianske-preukazy-este-v-tomto-roku/

CyberChef

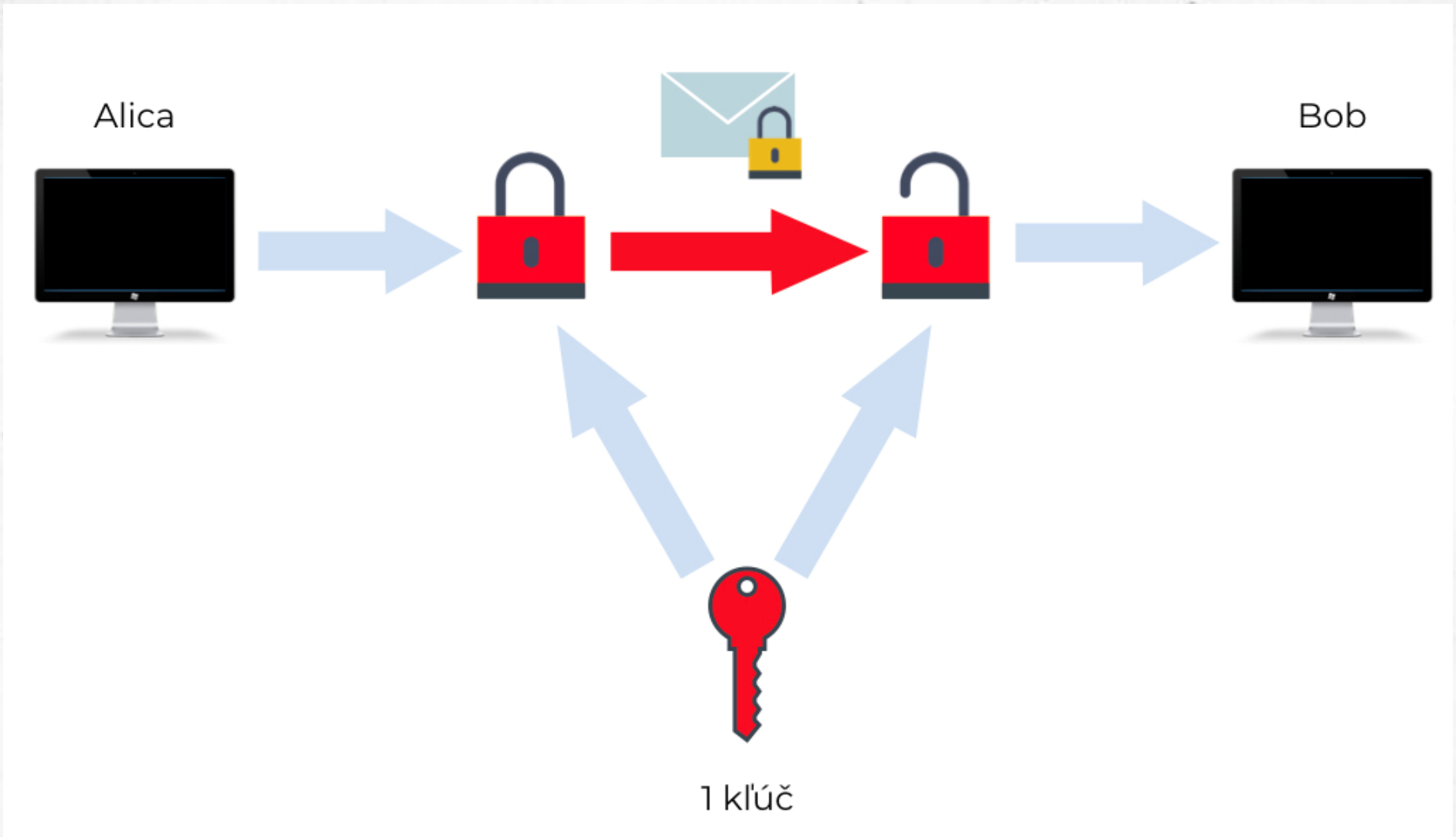
https://gchq.github.io/CyberChef/



Kryptografia



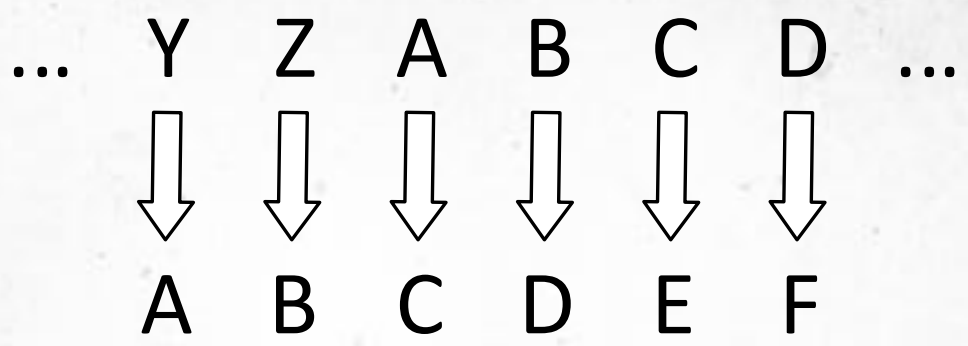
Symetrická kryptografia (I.)



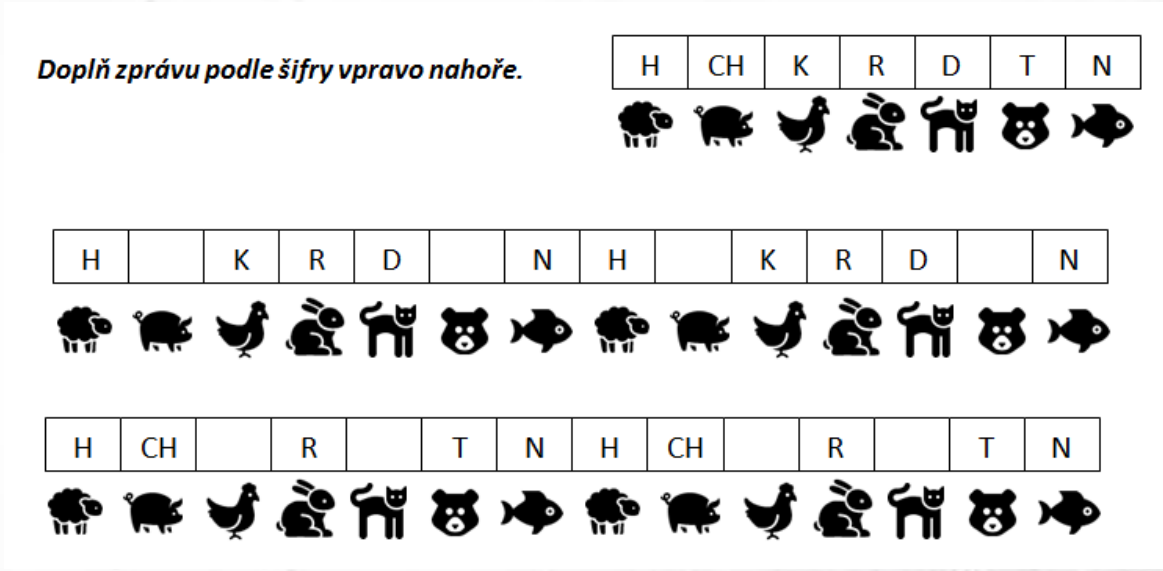
Symetrická kryptografia (II.)

Caesarova šifra a posuvná šifra

- Abecedný posun o fixný počet znakov = kľúč
- Ak je fixne nastavená „dĺžka posunu“ na 3, hovoríme o pôvodnej Caesarovej šifre



- **Substitučná šifra**

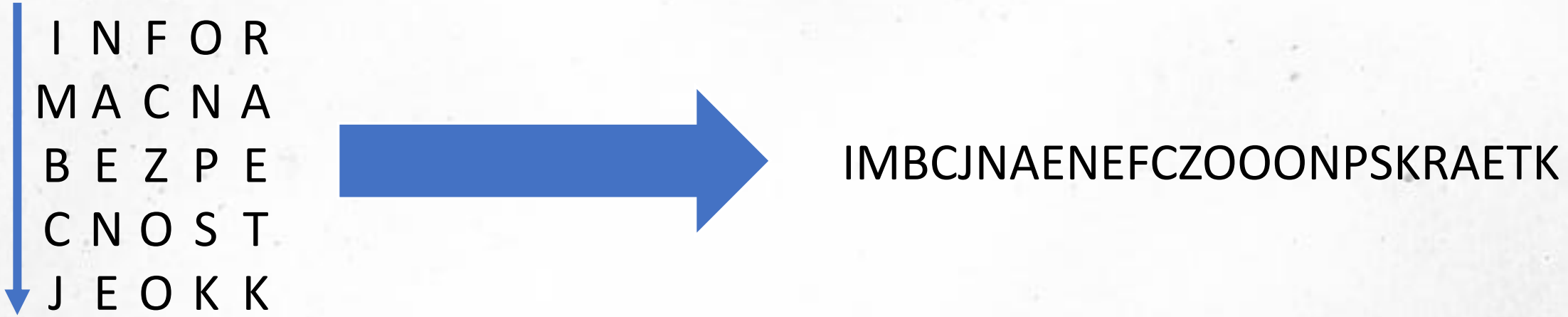


Zdroj: https://eschovka.cz/product/?pid=577

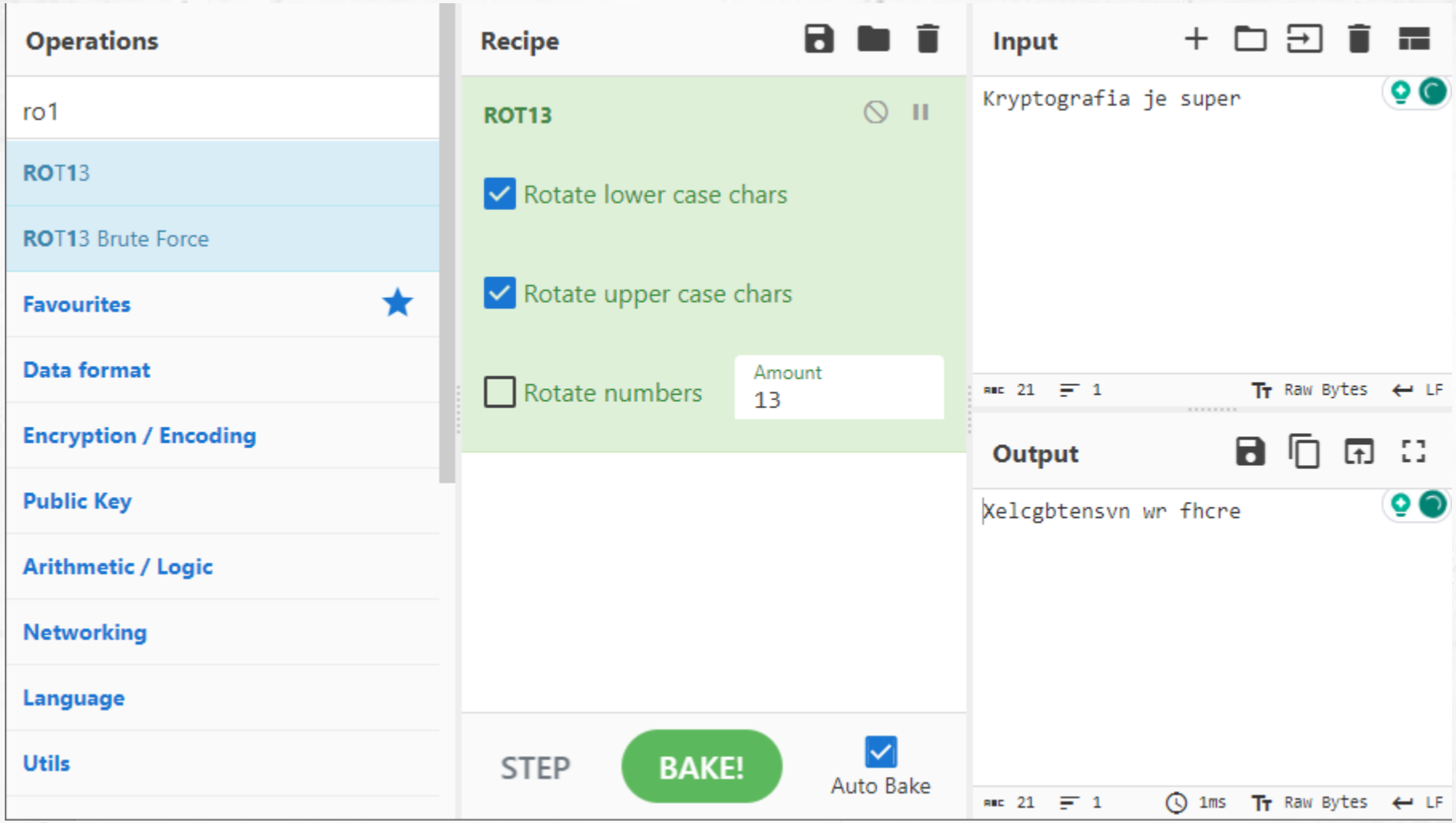
Symetrická kryptografia (III.)

Transpozičná šifra

- Prehodenie poradia znakov
- Napíšeme text do obdĺžnika fixnej dĺžky a transponujeme
- Zvolíme k, veľkosť bloku ako kľúč



Symetrická kryptografia (IV.)



Zdroj: https://gchq.github.io/CyberChef/

Symetrická kryptografia (V.)

Elektronické služby Úradu KSK sú dočasne nefunkčné

Košický samosprávny kraj sa za dočasný výpadok služieb ospravedlňuje, dôvodom je kybernetický bezpečnostný incident.

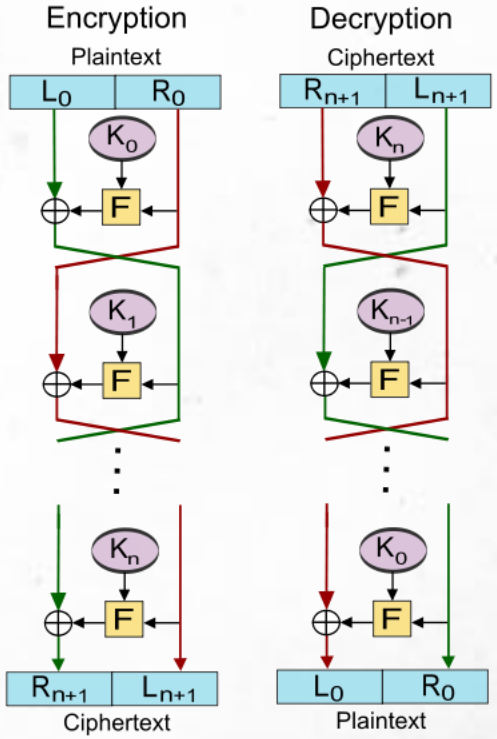
Úrad Košického samosprávneho kraja zaznamenal v utorok 5. septembra vo svojom počítačovom systéme nezvyčajné aktivity, ktoré boli vyhodnotené ako kybernetický bezpečnostný incident. Rovnako ako pri kybernetickom útoku z októbra 2021 malo ísť o tzv. ransomvér, teda druh škodlivého programu, ktorý dokáže uzamknúť zariadenie a zašifrovať jeho obsah.

!!! READ THIS - IMPORTANT !!!.txt - Notepad

File Edit Format View Help

```
<<<<<<<<<<<<<<<<<<<< YOUR FILES ARE ENCRYPTED! >>>>>>>>>>>>>>>>>>>>

SORRY! All personal files on your computer are encrypted.
File contents are encrypted with random key (AES-256; ECB mode).
Random key is encrypted with RSA public key (2048 bit).

We STRONGLY RECOMMEND you NOT to use any "decryption tools".
These tools can damage your data, making recover IMPOSSIBLE.
```

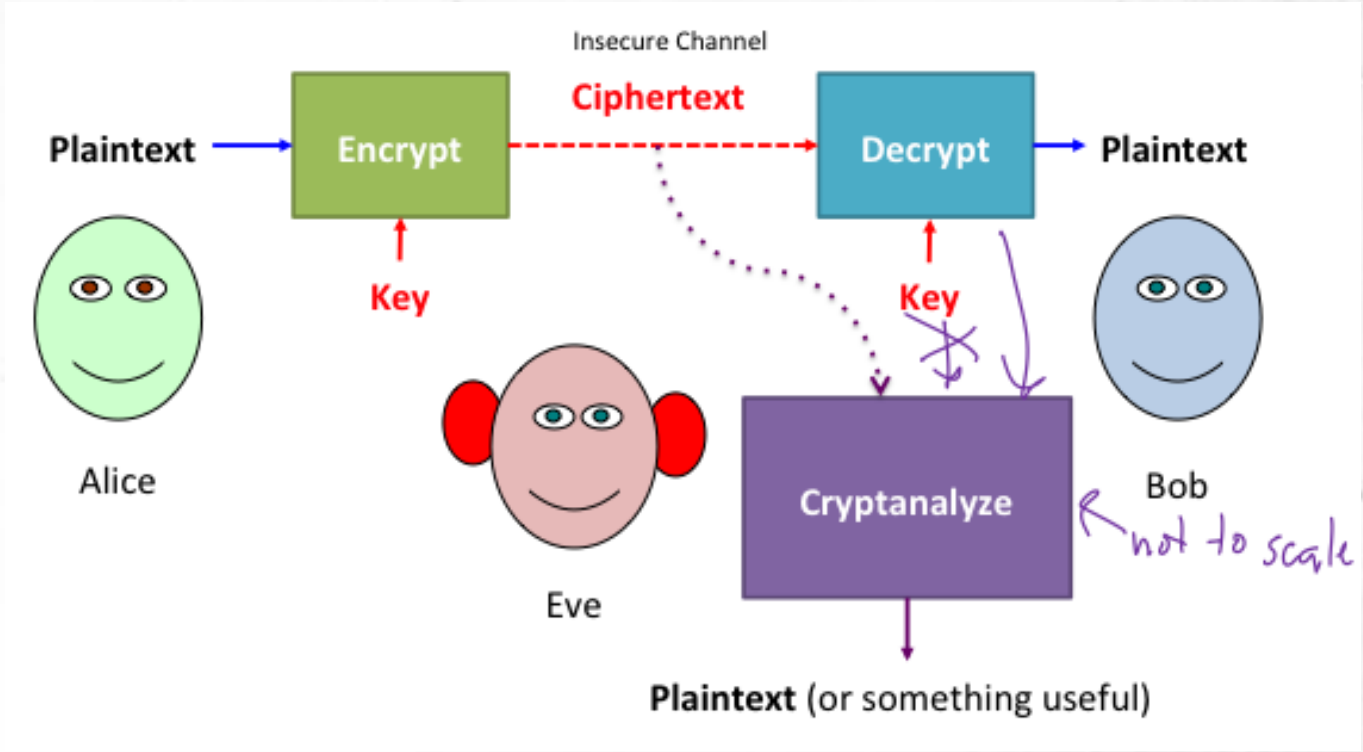
- **AES - Rijndael**
  - Bloková šifra
  - Pevná dĺžka bloku 128 bitov
  - Dĺžka kľúča 128,192,256 bitov



Zdroj: https://en.m.wikipedia.org/wiki/File:Feistel_cipher_diagram_en.svg, https://www.pcrisk.com/removal-guides/10766-aes256-ransomware

Kryptoanalýza (I.)

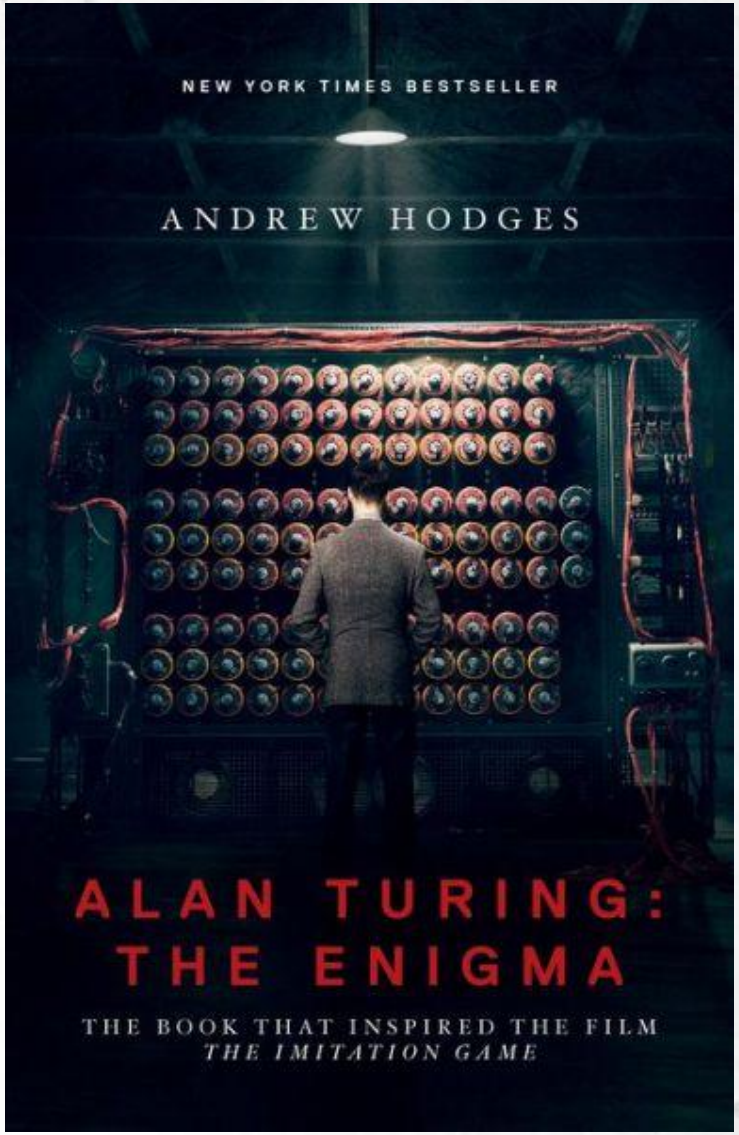
- Dĺžka textu, frekvencia, medzery
  - Predložky, spojky
- Jazyk textu – výhoda
- Ak poznáme prefix textu
  - Každá správa začína/končí na ...
  - Enigma – 3 písmená rovnaké v dennom kóde (xxx, ddd) - dešifrovanie



Zdroj: https://www.cs.virginia.edu/~evans/crypto/day1-cryptanalysis.html

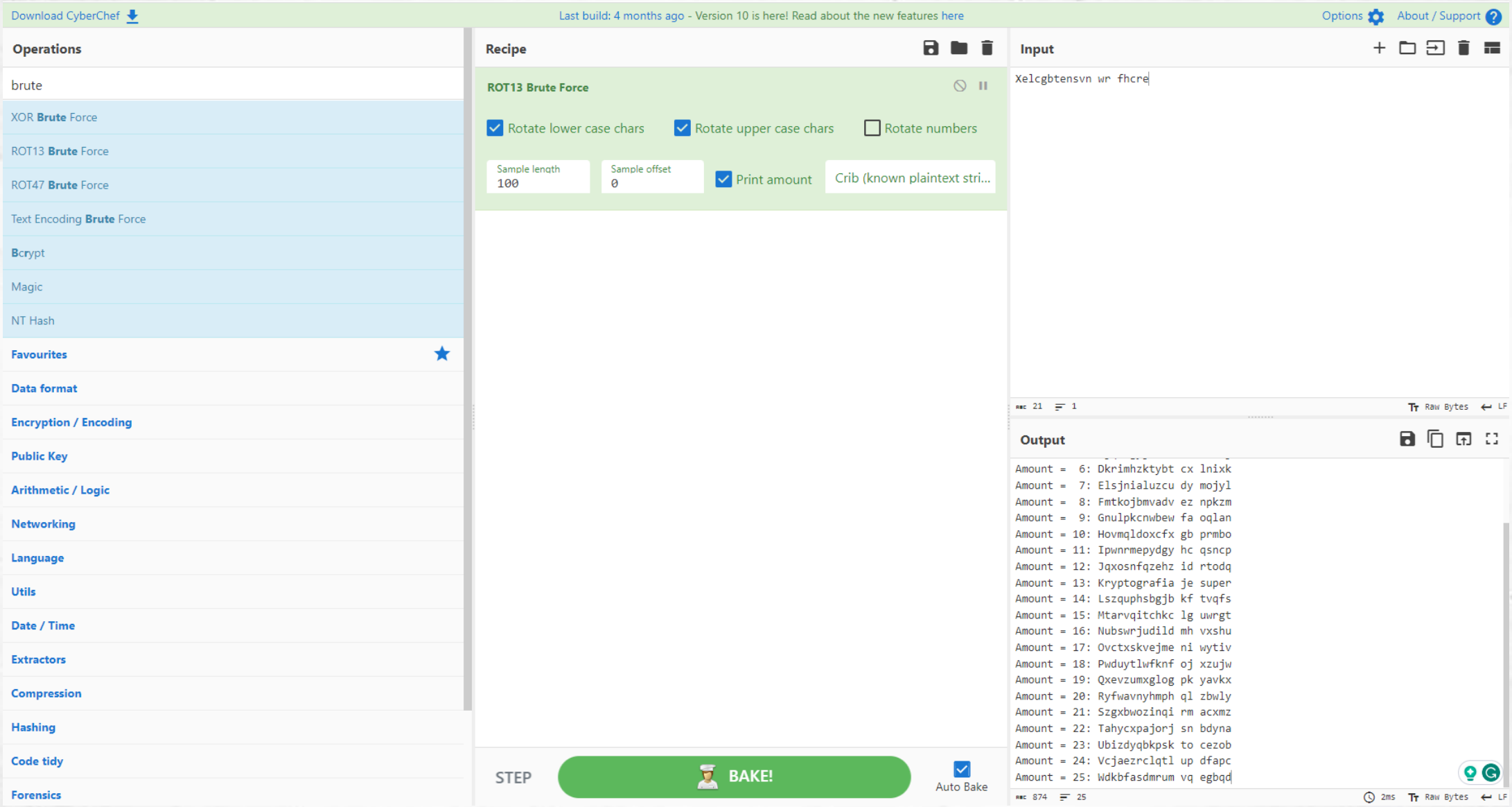
Kryptoanalýza (II.)

- **COA** – ciphertext only attack
  - Útok len so znalosťou šifrového textu
- **KPA** – known-plaintext attack
  - Útok so znalosťou otvoreného textu
- **CPA** – chosen-plaintext attack
  - Útok s možnosťou voľby otvoreného textu
- **CCA** – chosen-ciphertext attack
  - Útok s možnosťou voľby šifrového textu
- Side channels attack



Zdroj: https://www.barnesandnoble.com/readouts/alan-turing-the-enigma-the-book-that-inspired-the-film-the-imitation-game-updated-edition/

Kryptoanalýza (III.)



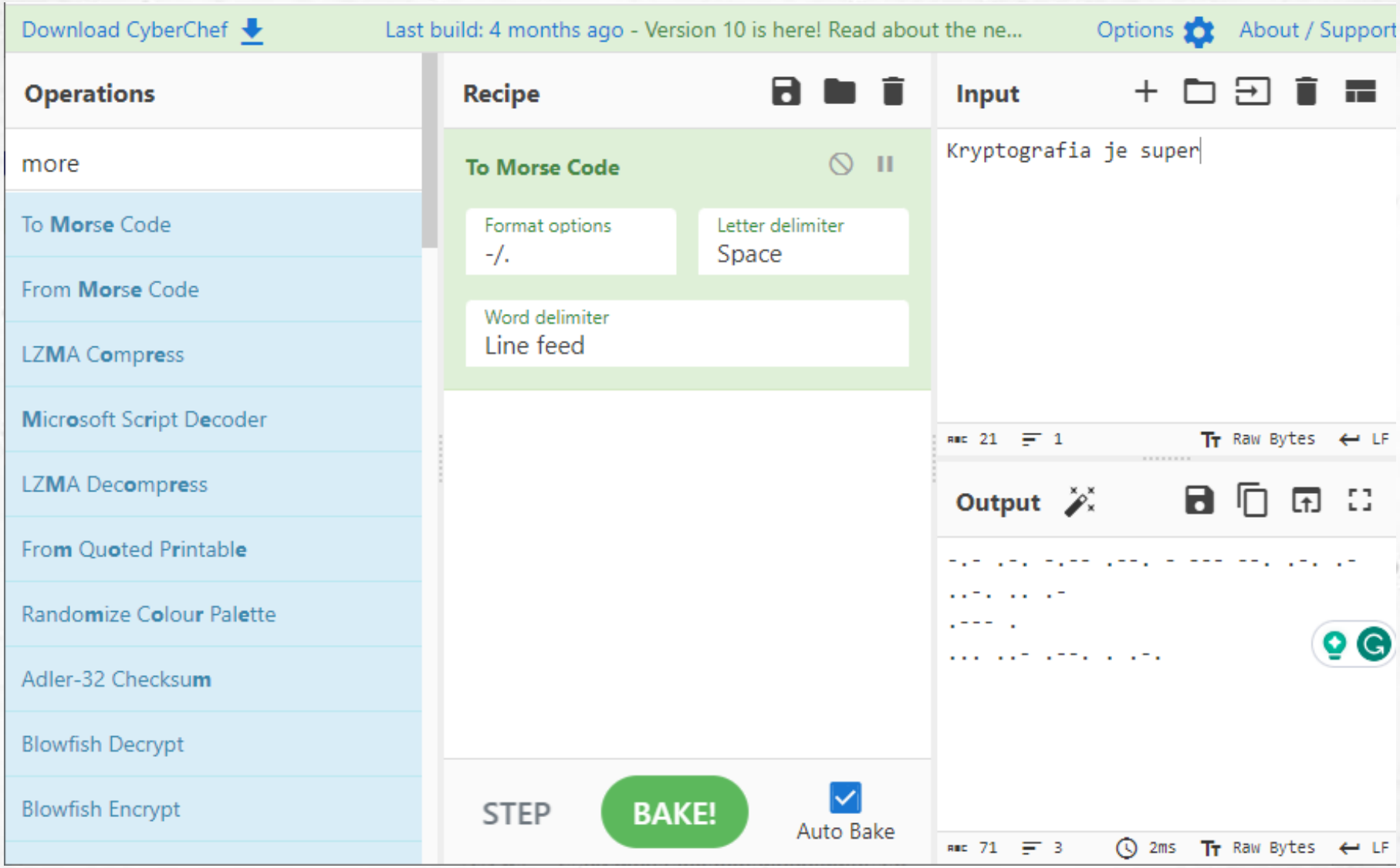
Zdroj: https://gchq.github.io/CyberChef/

Kryptografia vs. kódovanie (I.)

- Kryptografia – tajomstvo
- Kódovanie – bez tajomstva
  - Poznáme „prevod“

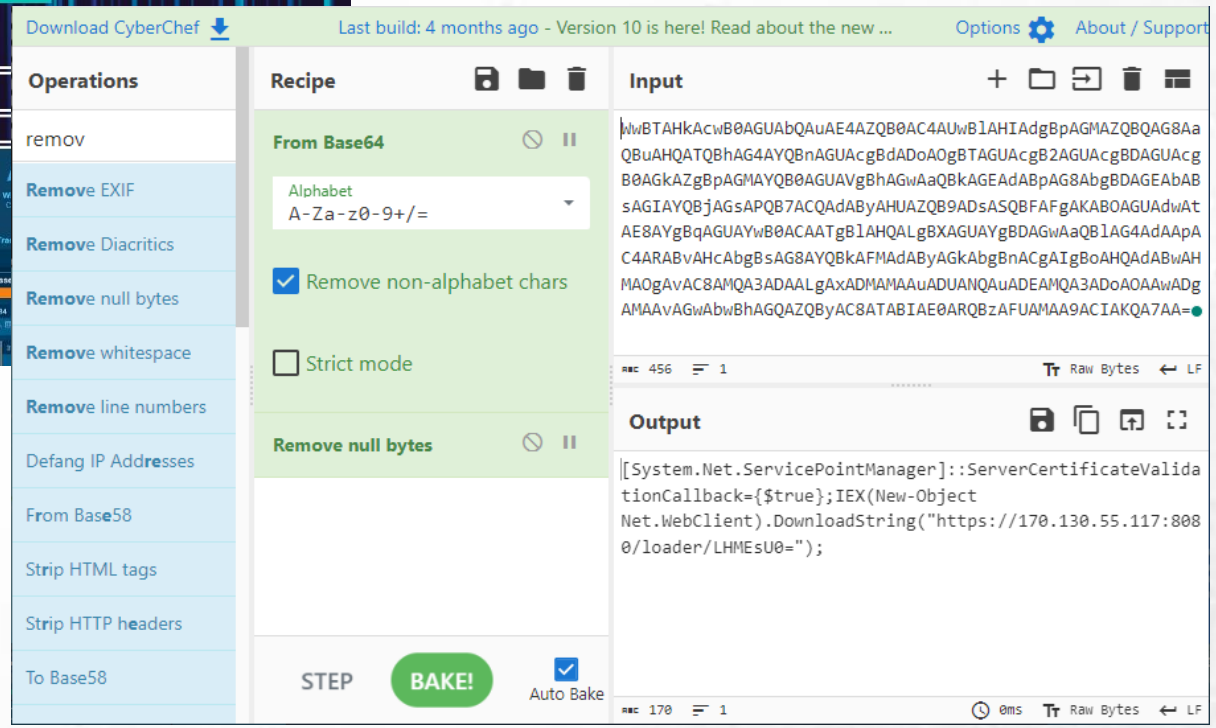
- KRYPTOGRAFIA NA UPJS JE SUPER! -> 4b525950544f47524146494120 4e412055504a53204a452053550455221
  - TEXT na HEX, pri ASCII kódovaní
- Arabský text - التشفير في UPJS رائع!
- Čínsky text - UPJS 的密碼學非常棒！
- Paleografia

Kryptografia vs. kódovanie (II.)



Zdroj: https://gchq.github.io/CyberChef/

Kryptografia vs. kódovanie (III.)



- https://app.any.run/tasks/3e092e4a-424e-4109-88a0-266e4038e397/
- Base64 kódovanie

Zdroj: https://gchq.github.io/CyberChef/

Hešovacie funkcie (I.)

O nás

CSIRT-UPJS je prvý akademický CSIRT v Slovenskej republike. Členmi tímu sú zamestnanci a študenti Centra informačných a komunikačných technológii, Prírodovedeckej a Právnickej fakulty. Dňa 14.12.2016 sme boli zaradení do zoznamu tímov na riešenie bezpečnostných incidentov vedeného medzinárodnou organizáciou TF-CSIRT (Trusted Introducer).

TF-CSIRT Trusted Introducer

Hlavnými činnosťami CSIRT tímu sú:

- vykonávanie proaktívnych (prevenčných) činností a reaktívnych činností smerujúcich k minimalizácií počtu bezpečnostných incidentov, resp. k zníženiu dopadu v prípade ich výskytu
- zvyšovanie bezpečnostného povedomia zamestnancov a študentov univerzity
- iné činnosti nevyhnutné k zabezpečeniu informačnej bezpečnosti univerzity.

Všetky informácie o našom tíme z tejto webovej stránky nájdete na jednom mieste v RFC-2350 dokumente.
K dispozícií je aj podpis dokumentu pre overenie.

O nás

CSIRT-UPJS je prvý akademický CSIRT v Slovenskej republike. Členmi tímu sú zamestnanci a študenti Centra informačných a komunikačných technológii, Prírodovedeckej a Právnickej fakulty. Dňa 14.12.2016 sme boli zaradení do zoznamu tímov na riešenie bezpečnostných incidentov vedeného medzinárodnou organizáciou TF-CSIRT (Trusted Introducer).

TF-CSIRT Trusted Introducer

Hlavnými činnosťami CSIRT tímu sú:

- vykonávanie proaktívnych (prevenčných) činností a reaktívnych činností smerujúcich k zvýšeniu počtu bezpečnostných incidentov, resp. k zníženiu dopadu v prípade ich výskytu
- zvyšovanie bezpečnostného povedomia zamestnancov a študentov univerzity
- iné činnosti nevyhnutné k zabezpečeniu informačnej bezpečnosti univerzity.

Všetky informácie o našom tíme z tejto webovej stránky nájdete na jednom mieste v RFC-2350 dokumente.
K dispozícií je aj podpis dokumentu pre overenie.

Zdroj: https://csirt.upjs.sk/#/o-nas

Hešovacie funkcie (II.)

O nás

CSIRT-UPJS je prvý akademický CSIRT v Slovenskej republike. Členmi tímu sú zamestnanci a študenti Centra informačných a komunikačných technológii, Prírodovedeckej a Právnickej fakulty. Dňa 14.12.2016 sme boli zaradení do zoznamu tímov na riešenie bezpečnostných incidentov vedeného medzinárodnou organizáciou TF-CSIRT (Trusted Introducer).

TF-CSIRT Trusted Introducer

Hlavnými činnosťami CSIRT tímu sú:

- vykonávanie proaktívnych (prevenčných) činností a reaktívnych činností smerujúcich k minimalizácií počtu bezpečnostných incidentov, resp. k zníženiu dopadu v prípade ich výskytu
- zvyšovanie bezpečnostného povedomia zamestnancov a študentov univerzity
- iné činnosti nevyhnutné k zabezpečeniu informačnej bezpečnosti univerzity.

Všetky informácie o našom tíme z tejto webovej stránky nájdete na jednom mieste v RFC-2350 dokumente.
K dispozícií je aj podpis dokumentu pre overenie.

O nás

CSIRT-UPJS je prvý akademický CSIRT v Slovenskej republike. Členmi tímu sú zamestnanci a študenti Centra informačných a komunikačných technológii, Prírodovedeckej a Právnickej fakulty. Dňa 14.12.2016 sme boli zaradení do zoznamu tímov na riešenie bezpečnostných incidentov vedeného medzinárodnou organizáciou TF-CSIRT (Trusted Introducer).

TF-CSIRT Trusted Introducer

Hlavnými činnosťami CSIRT tímu sú:

- vykonávanie proaktívnych (prevenčných) činností a reaktívnych činností smerujúcich k zvýšeniu počtu bezpečnostných incidentov, resp. k zníženiu dopadu v prípade ich výskytu
- zvyšovanie bezpečnostného povedomia zamestnancov a študentov univerzity
- iné činnosti nevyhnutné k zabezpečeniu informačnej bezpečnosti univerzity.

Všetky informácie o našom tíme z tejto webovej stránky nájdete na jednom mieste v RFC-2350 dokumente.
K dispozícií je aj podpis dokumentu pre overenie.

Zdroj: https://csirt.upjs.sk/#/o-nas

Hešovacie funkcie (III.)

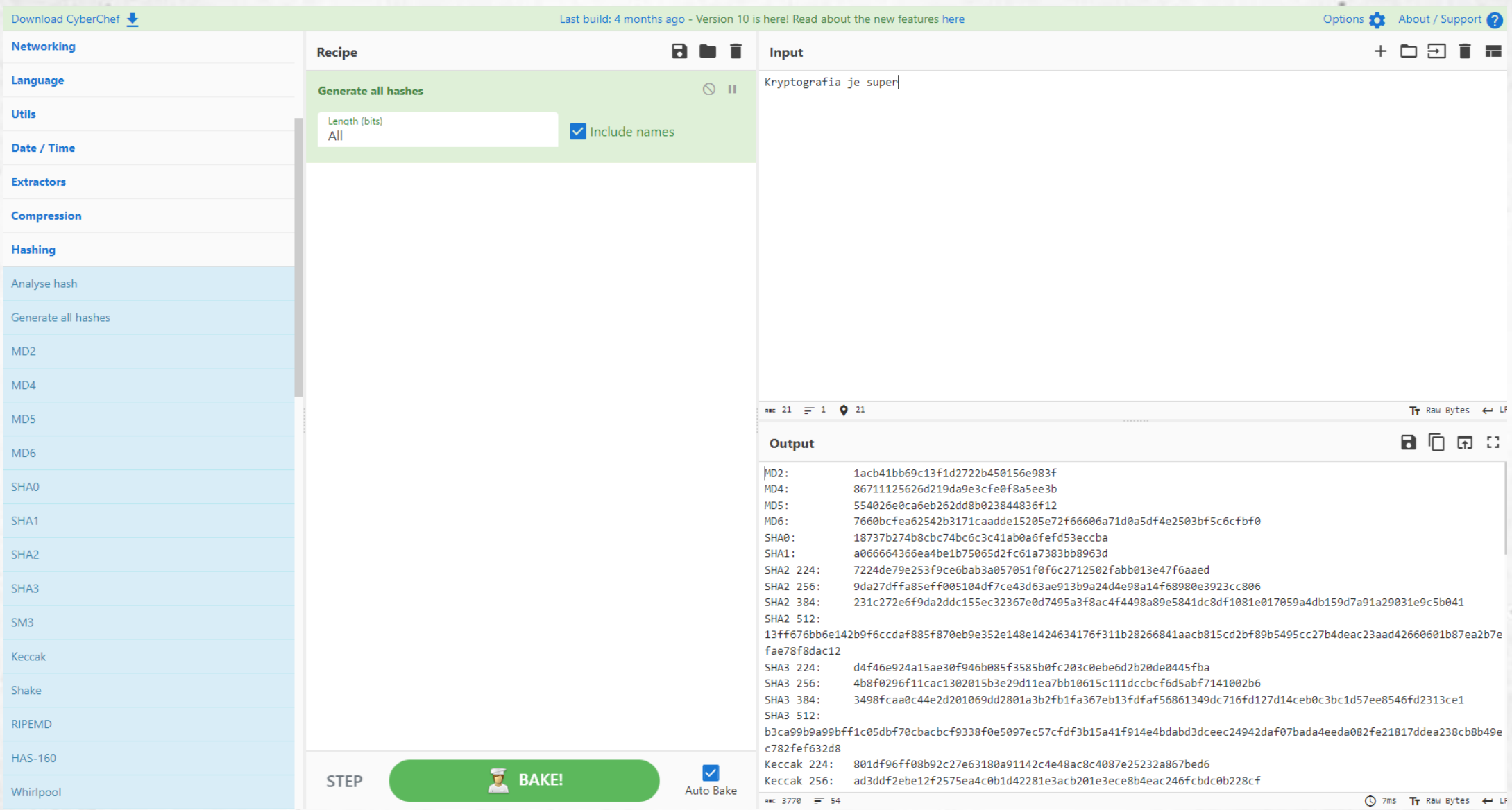
- **Hešovacia funkcia** je jednosmerná funkcia, ktorá pre reťazec ľubovoľnej dĺžky vráti reťazec pevnej dĺžky.
- Známe hešovanie funkcie:
  - MD5 (Message-digest 5)
  - SHA-1 (Secure hash algorithm 1)
  - SHA-2 (256/384/512)

Zdroj: https://www.giallozafferano.com/recipes/torta-tenerina-moist-chocolate-cake.html

Vstup: Kryptografia je super

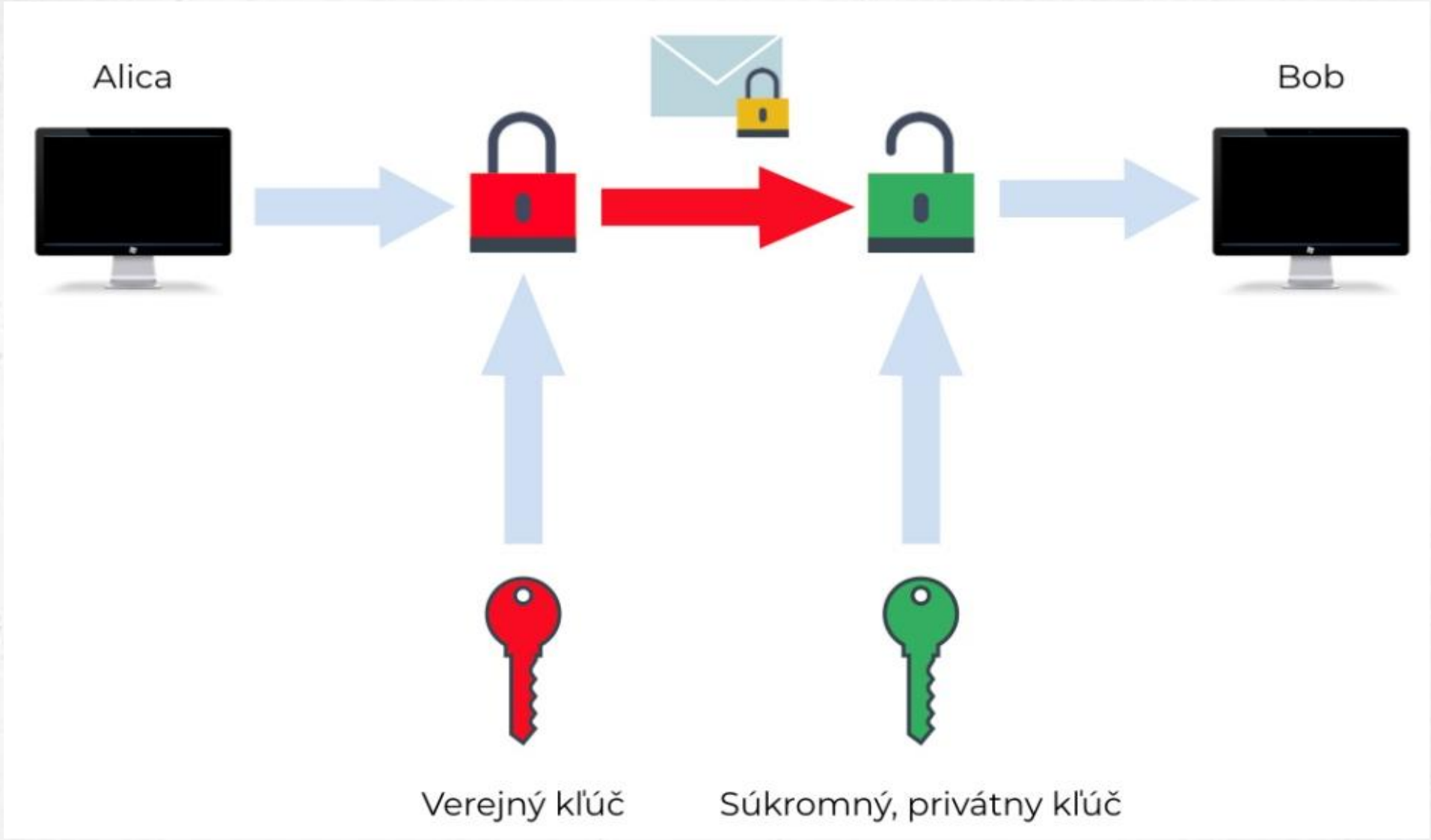
- MD5: 554026e0ca6eb262dd8b023844836f12
- SHA0: 18737b274b8cbc74bc6c3c41ab0a6fefd53eccba
- SHA2 256: 9da27dffa85eff005104df7ce43d63ae913b9a24d4e98a14f68980e3923cc8
- LM Hash: 06F6B1AA290EA7E0A47539F1B0511046
- NT Hash: 26D6089127567D17C9E5FD1554F57BA0

Hešovacie funkcie (IV.)



Zdroj: https://gchq.github.io/CyberChef/

Asymetrická kryptografia (I.)



Asymetrická kryptografia (II.)

RSA (Rivest–Shamir–Adleman)

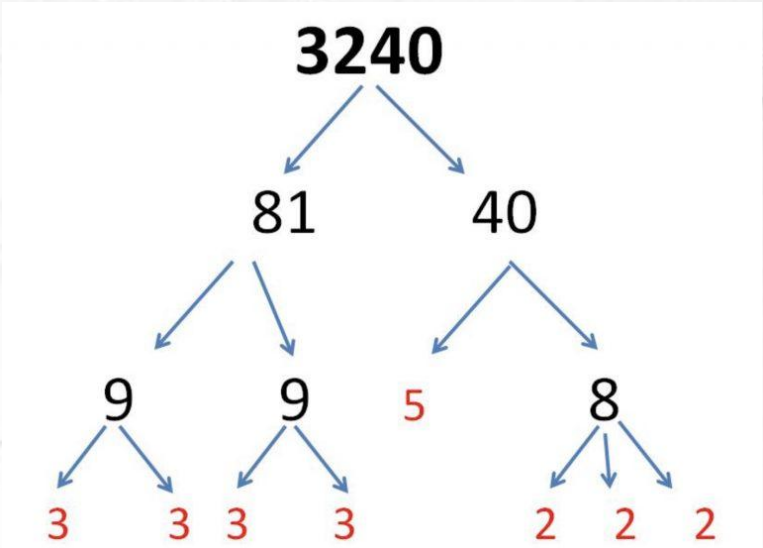
- Problém faktorizácie

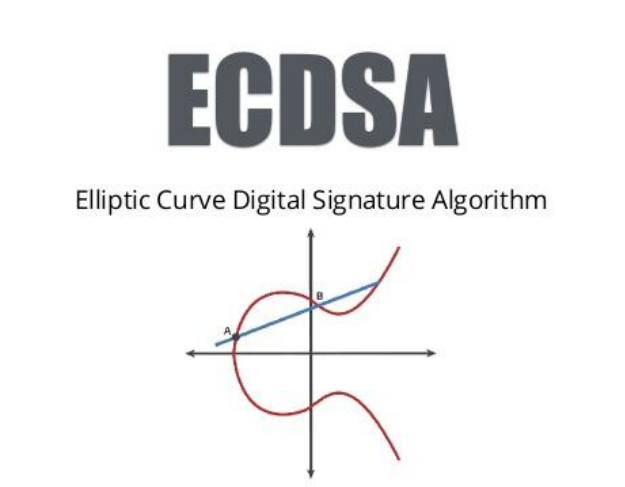
ElGamal

- Problém diskrétneho logaritmu

ECDSA

- Eliptické krivky



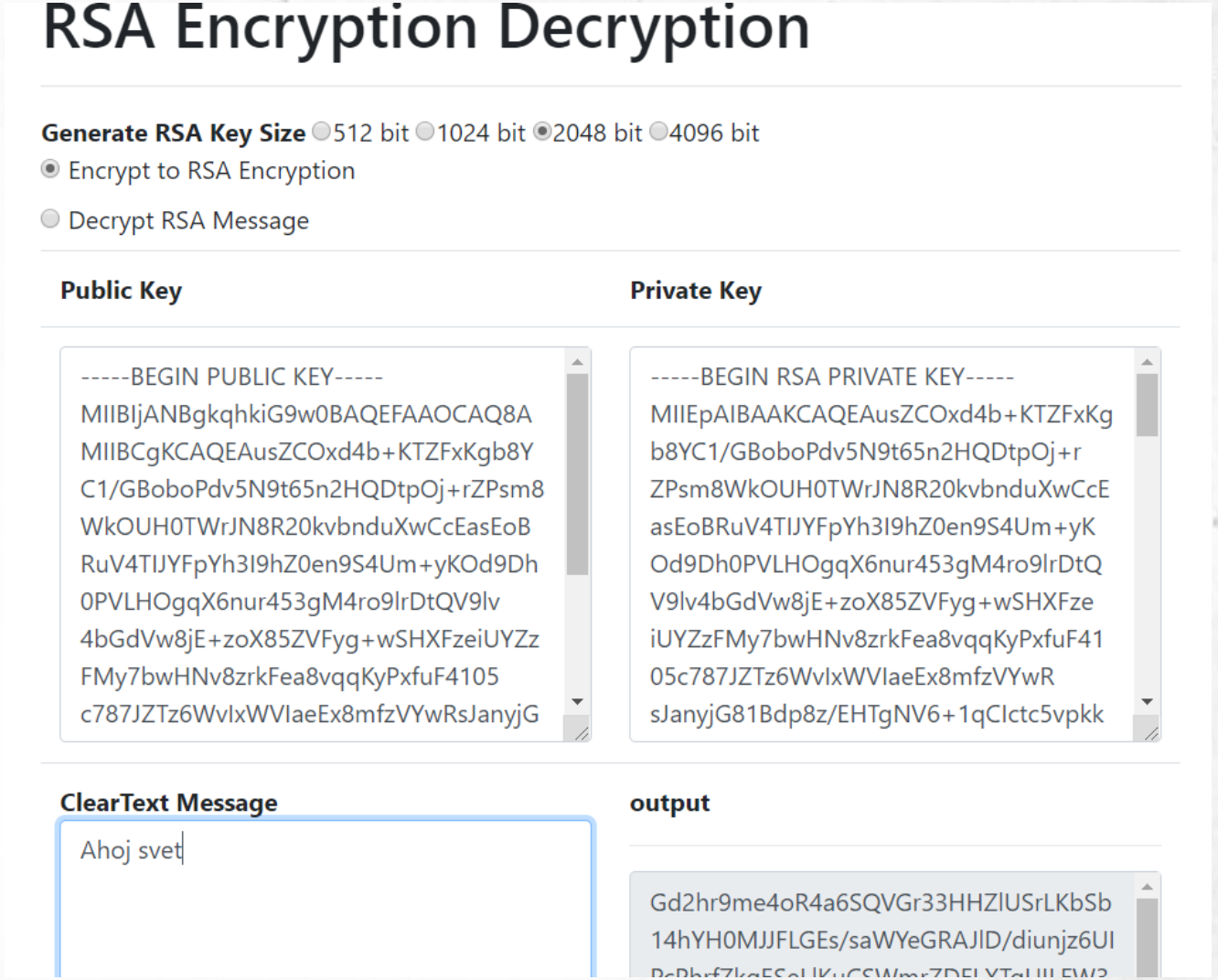


Zdroj: https://www.explosion.com/138783/what-is-prime-factorization/, https://metamug.com/article/sign-verify-digital-signature-ecdsa-java.html

Asymetrická kryptografia (III.)

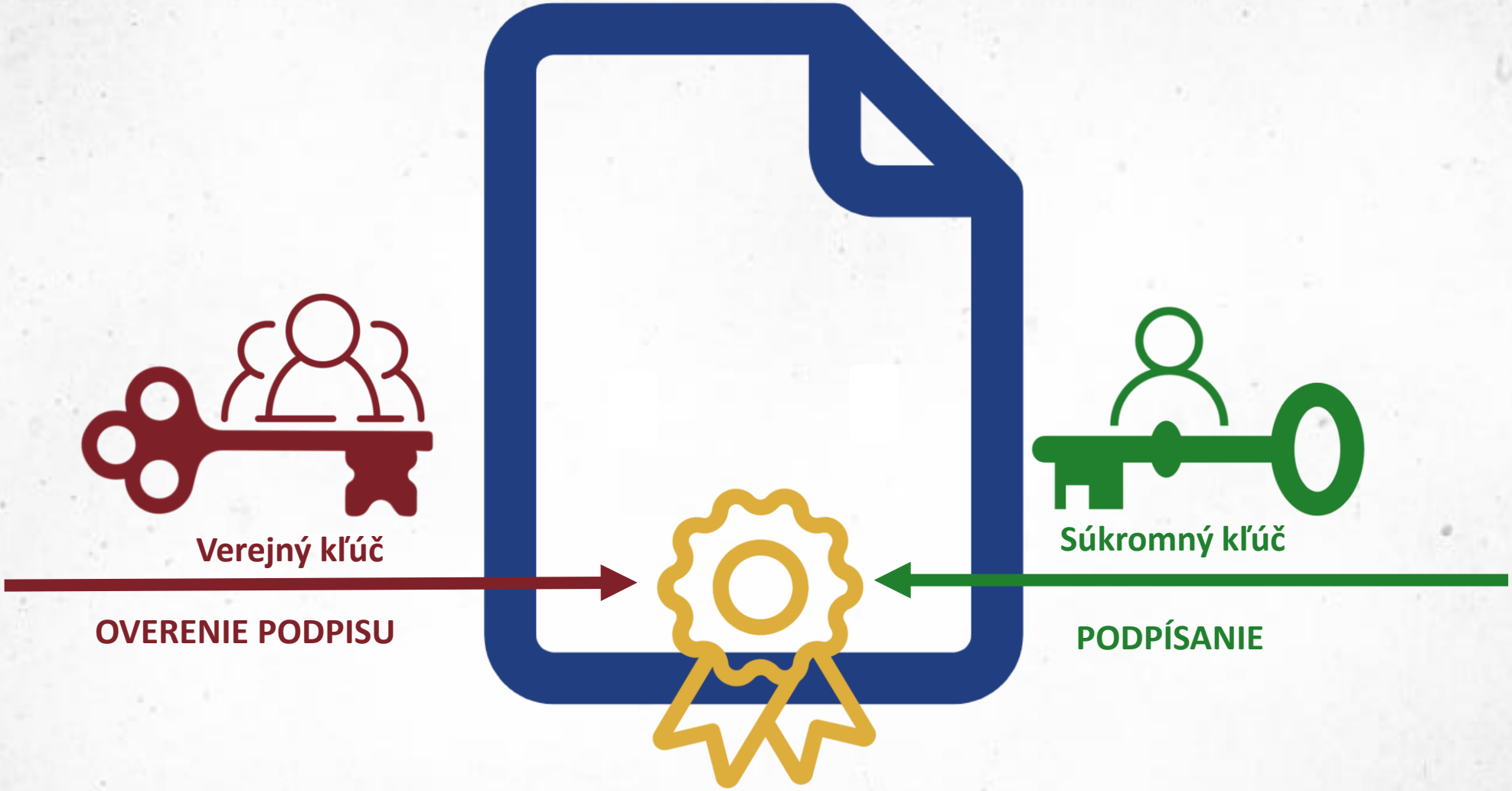
Online nástroj

- https://8gwifi.org/rsafunctions.jsp
- https://shorturl.at/JK65n
- RSA asymetrická šifra

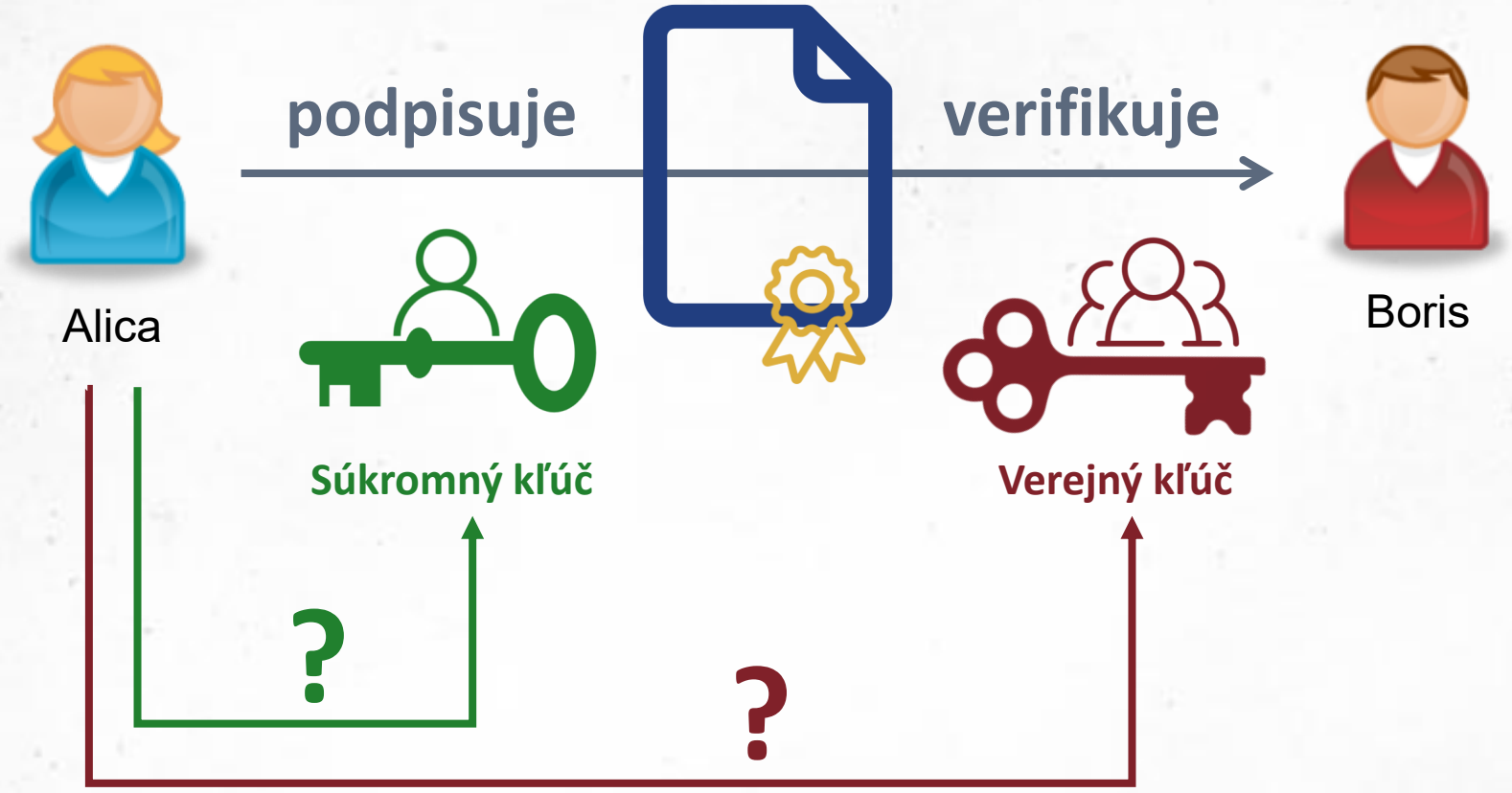


Šifrovanie vs. podpisovanie (I.)

Šifrovanie vs. podpisovanie (II.)



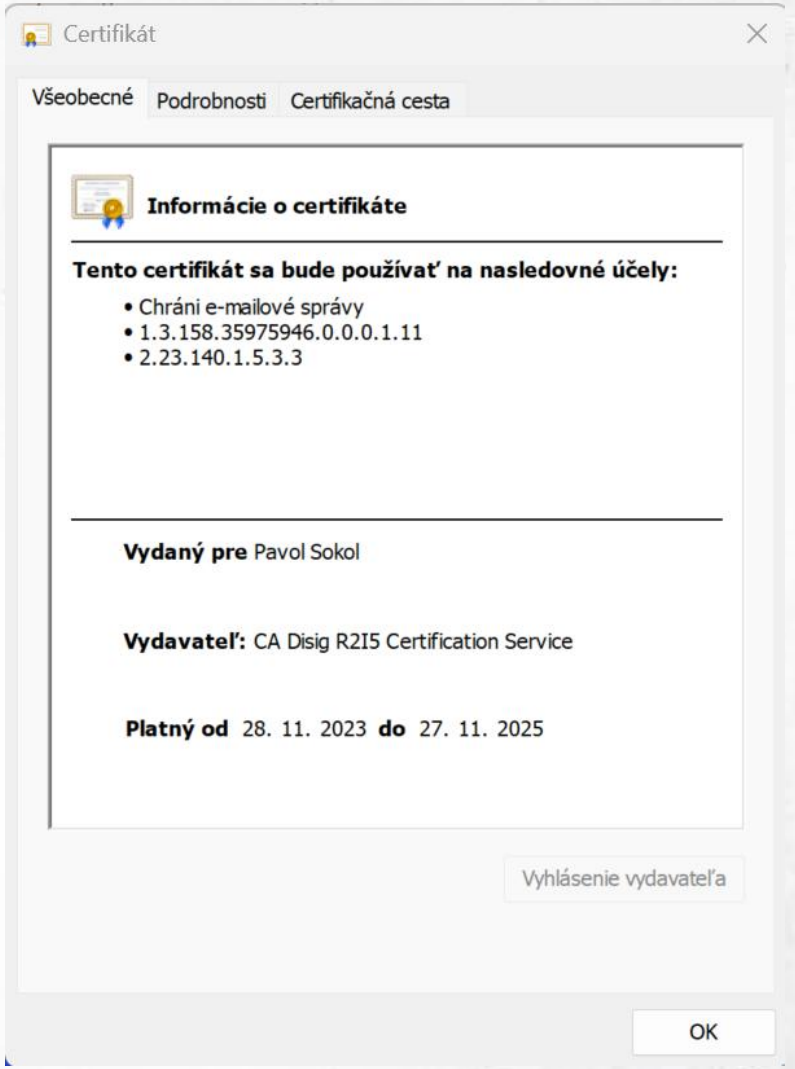
Certifikát (I.)



Certifikát (II.)

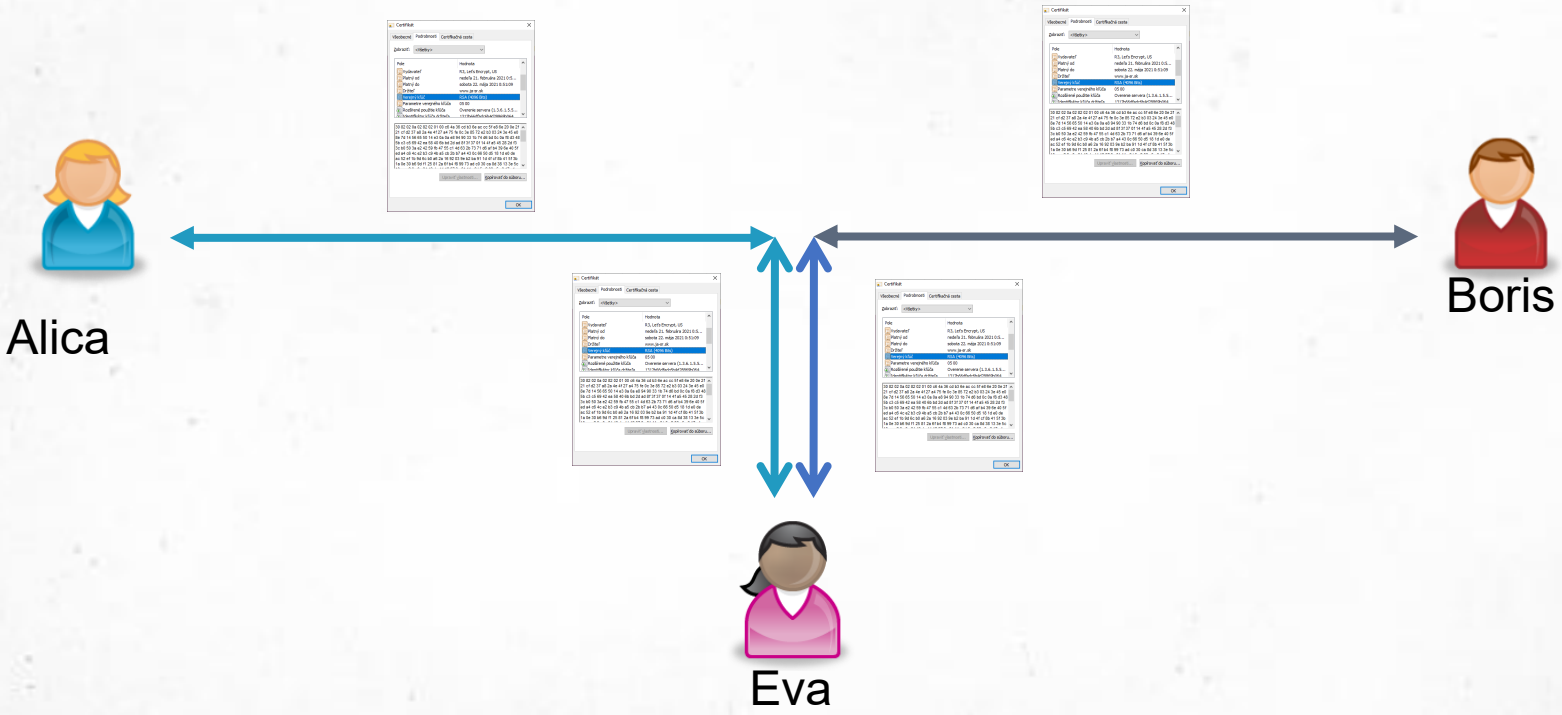
Certifikát (III.)

- **Certifikáty** zväzujú verejný kľúč a vlastníka kľúča.
- **Certifikát pre elektronický podpis** je elektronické osvedčenie, ktoré spája údaje na validáciu elektronického podpisu s fyzickou osobou a potvrdzuje aspoň jej meno alebo pseudonym (Nariadenie eIDAS)



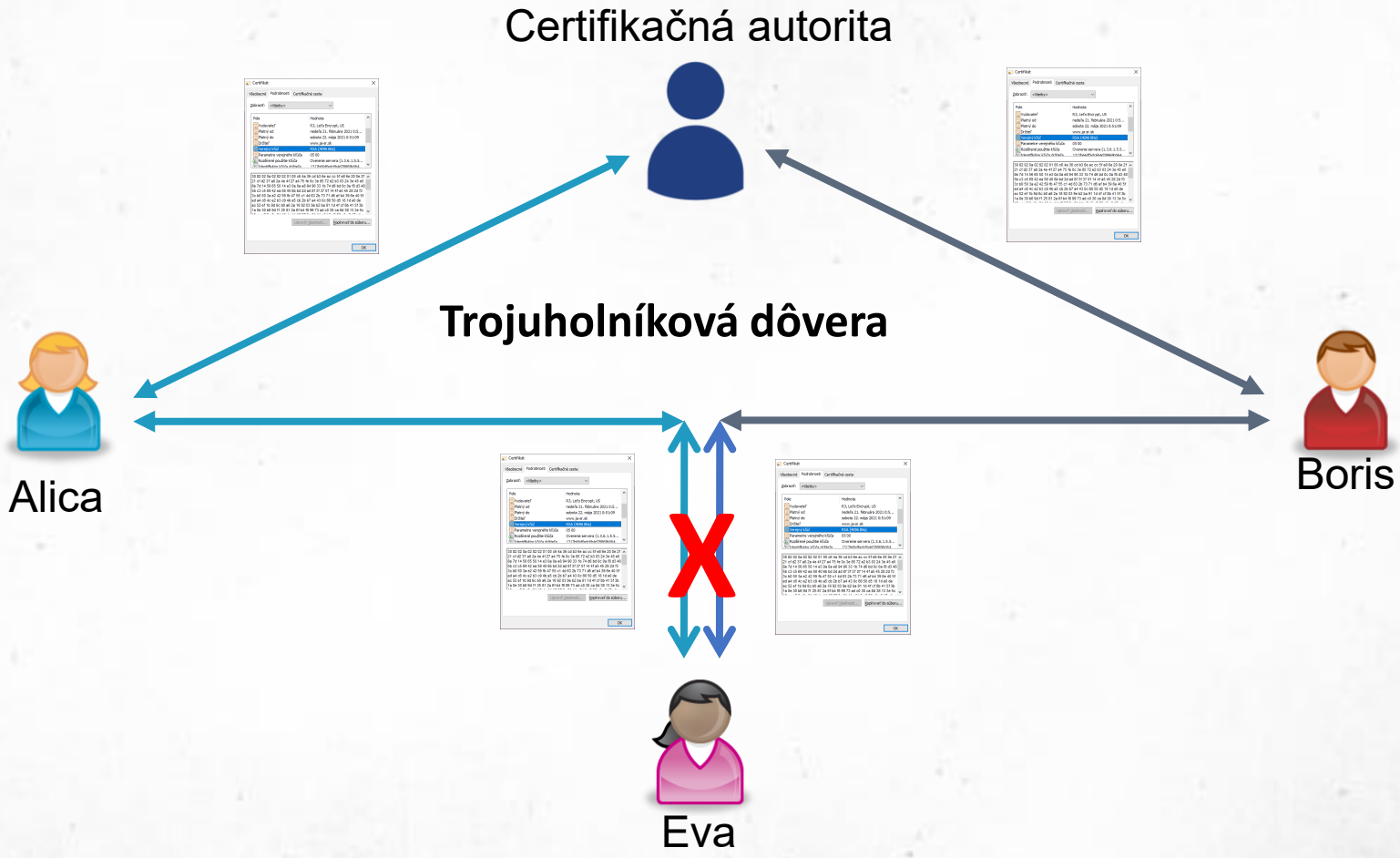
Certifikačná autorita (I.)

- Problém so správou certifikátov
- útok – útočník v strede (man in the middle attack)
- Potreba autority – 3. nezávislej strany



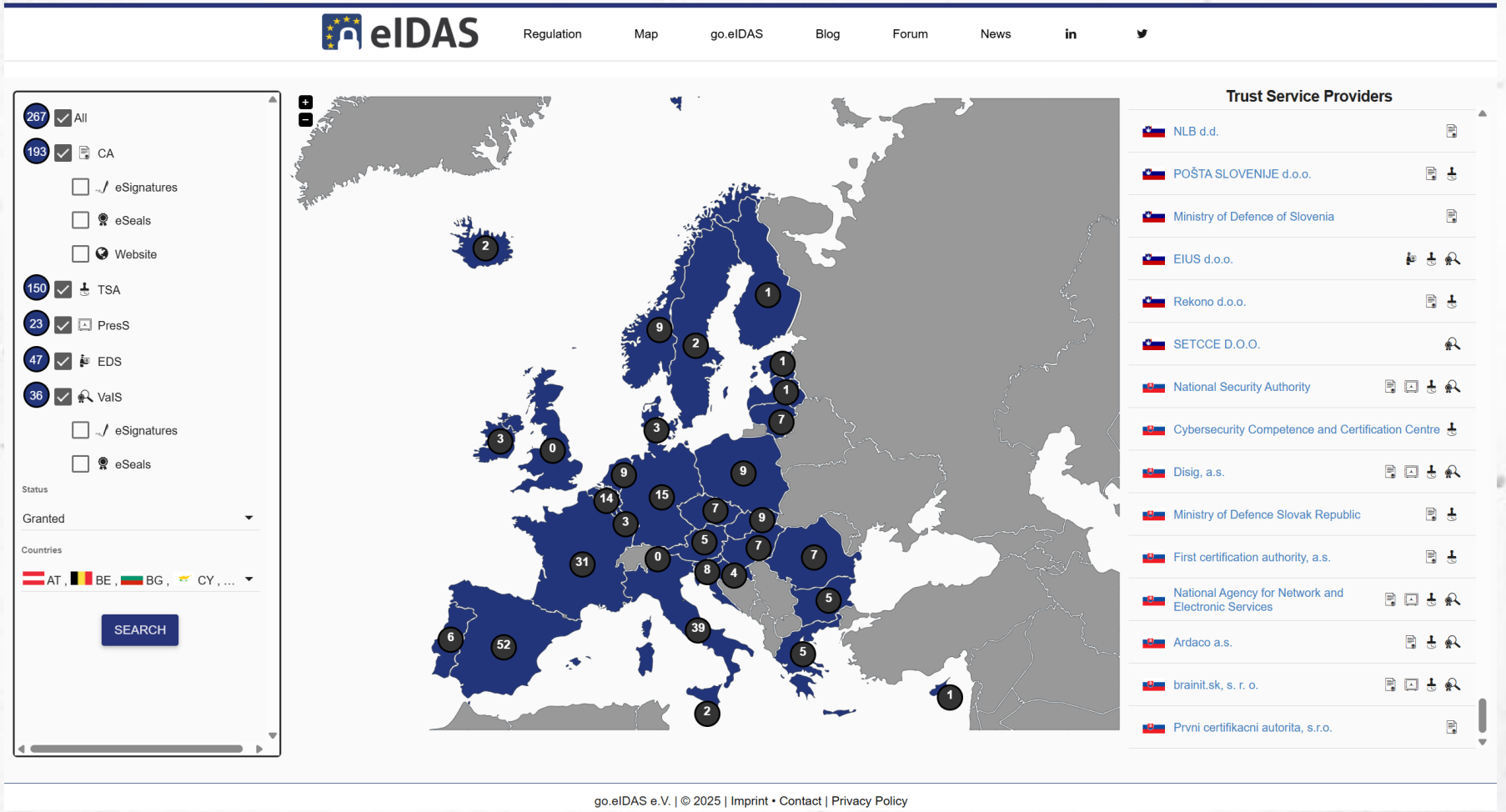
Certifikačná autorita (II.)

- Nezávislá autorita – spravuje certifikáty – vydáva, overuje, ruší ...



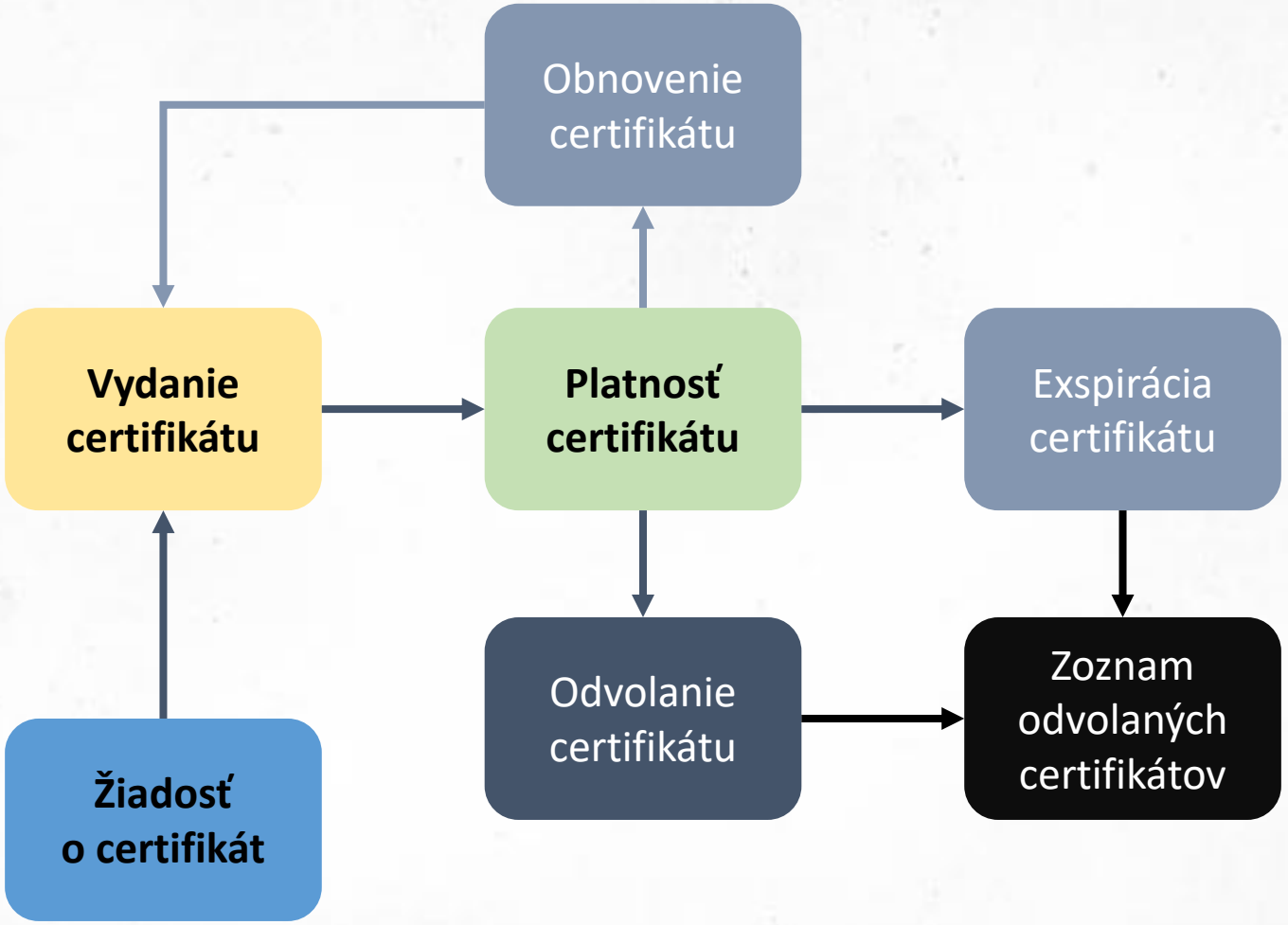
Certifikačná autorita (III.)

- Poskytovatelia dôveryhodných služieb = certifikačné autority + ...



Zdroj: https://www.eid.as/tsp-map/#/

Životný cyklus certifikátu (I.)



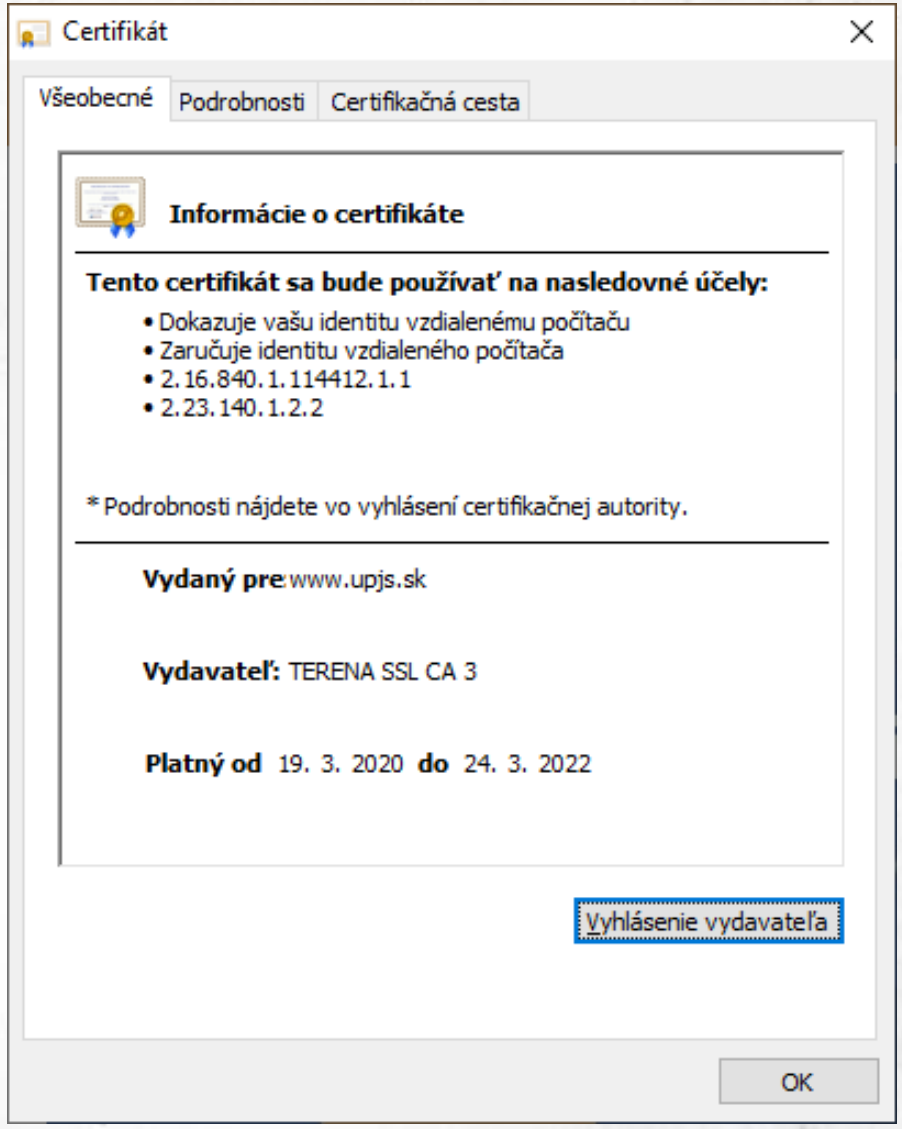
Životný cyklus certifikátu (II.)

Platnosť certifikátov

- položky **Not before** (od) a **Not after** (do)
- **overenie platnosti certifikátu** (doba, CRL, certifikačná cesta)

- Platnosť certifikátu sa môže ukončiť 3 spôsobmi:
  - **ukončením platnosti certifikátu**
  - **obnovením certifikátu**
  - **zrušením certifikátu**

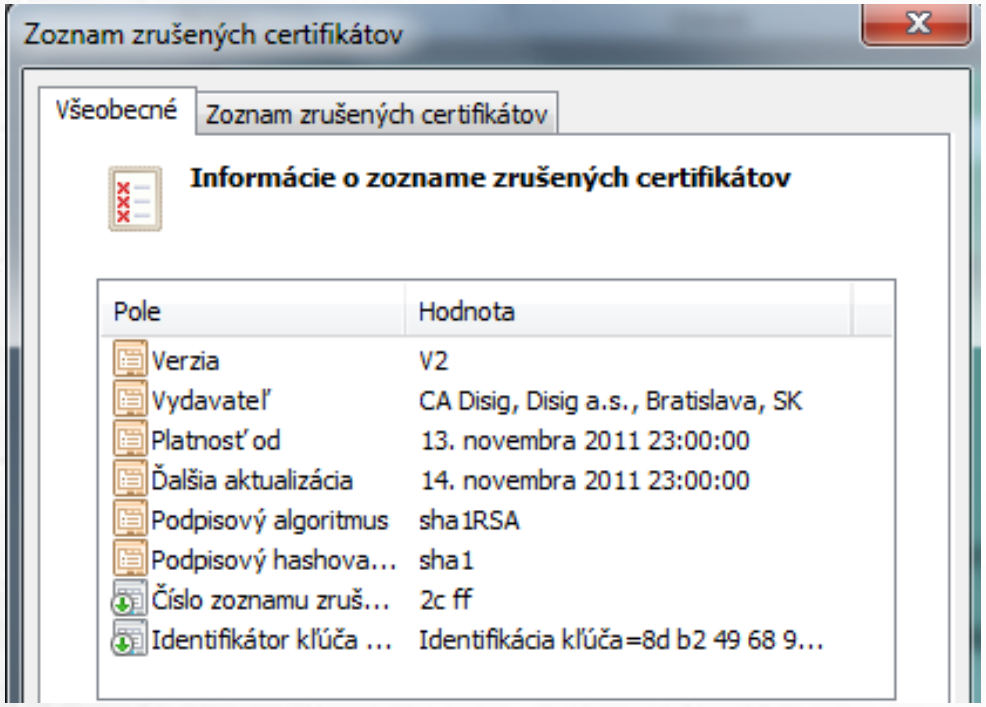
- Subjekty:
  - **podpisovateľ** elektronického podpisu
  - **overovateľ** elektronického podpisu

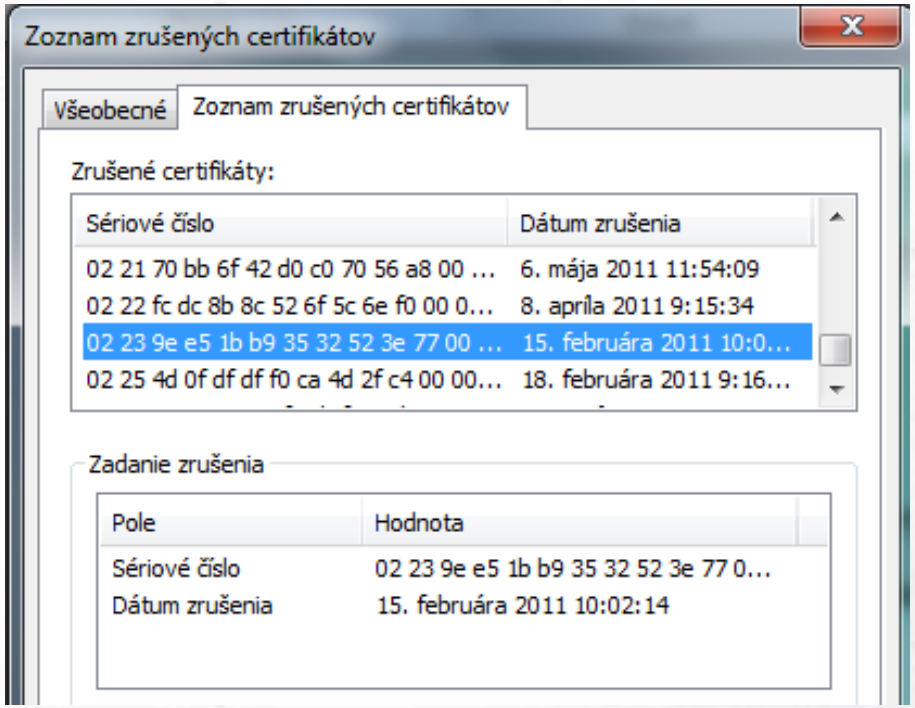


Životný cyklus certifikátu (III.)

Zoznam zrušených certifikátov - certificate revocation list (CRL)

- elektronický dokument, ktorým vydavateľ certifikátov, ktorý spravuje tieto certifikáty, oznamuje predčasné ukončenie ich platnosti.
- periodicita vydávania
- štandard RFC 5280





Podpis (I.)

- latinského slovo „signum“
- podpis priestorovo a obsahovo uzaviera nielen listinu, ale i samotný písomný právny úkon
- Podpis plní nasledujúce funkcie:
  - **označovaciu funkciu** – označuje osobu, ktorá vykonala právny úkon
  - **deklaračnú funkciu** – potvrdzuje obsah prejav vôle danej osoby
  - **dôkaznú funkciu** – potvrdzuje, že daný prejav vôle bol daný

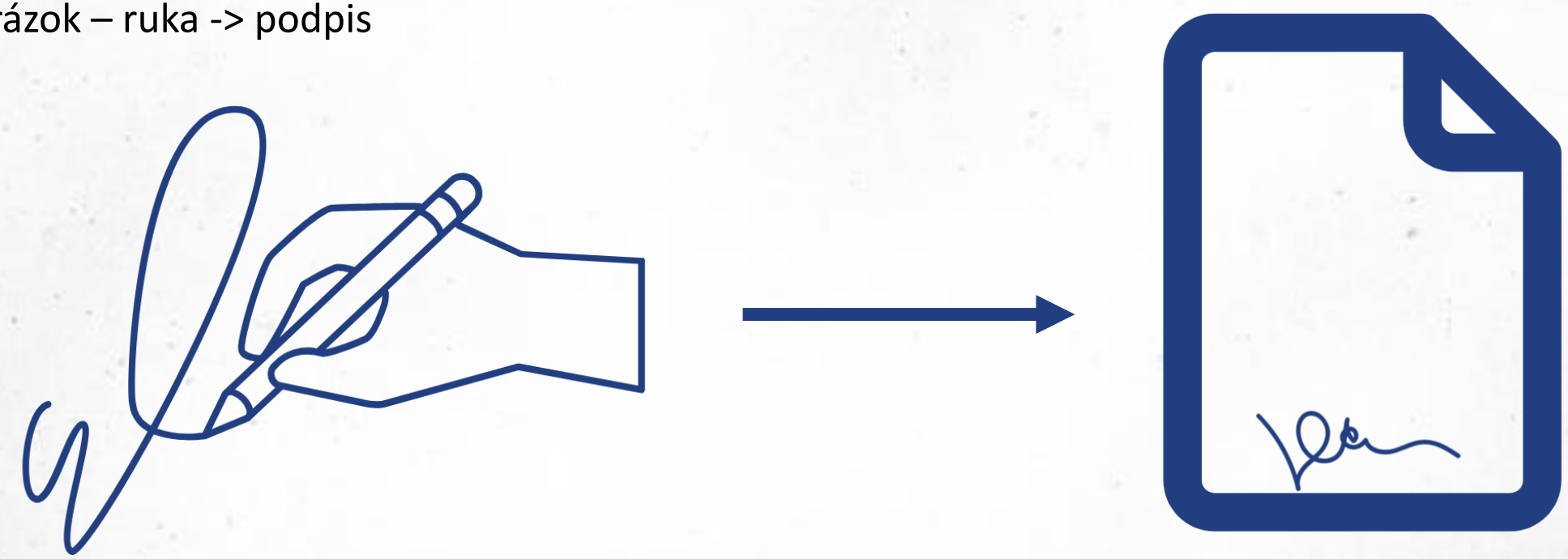
Podpis (II.)

V právnej teórii a praxi sa rozoznáva niekoľko druhov podpisov:

- **vlastnoručný podpis**
- **overený, resp. osvedčený podpis**
  - udelenie oprávnenia na prístup a disponovanie s elektronickou schránkou
- **podpis nahradený mechanickými prostriedkami**
  - nahradenie podpisu pomocou pečiatky či faksimili, naskenovanie podpisu
- **elektronický podpis (aj zdokonalený, kvalifikovaný)**

Podpis (III.)

- Prostriedok na vytvorenie podpisu vs. Výsledok procesu písania (vytvorenia podpisu)
- Prostriedok – ruka, resp. končatina
- Obrázok – ruka -> podpis

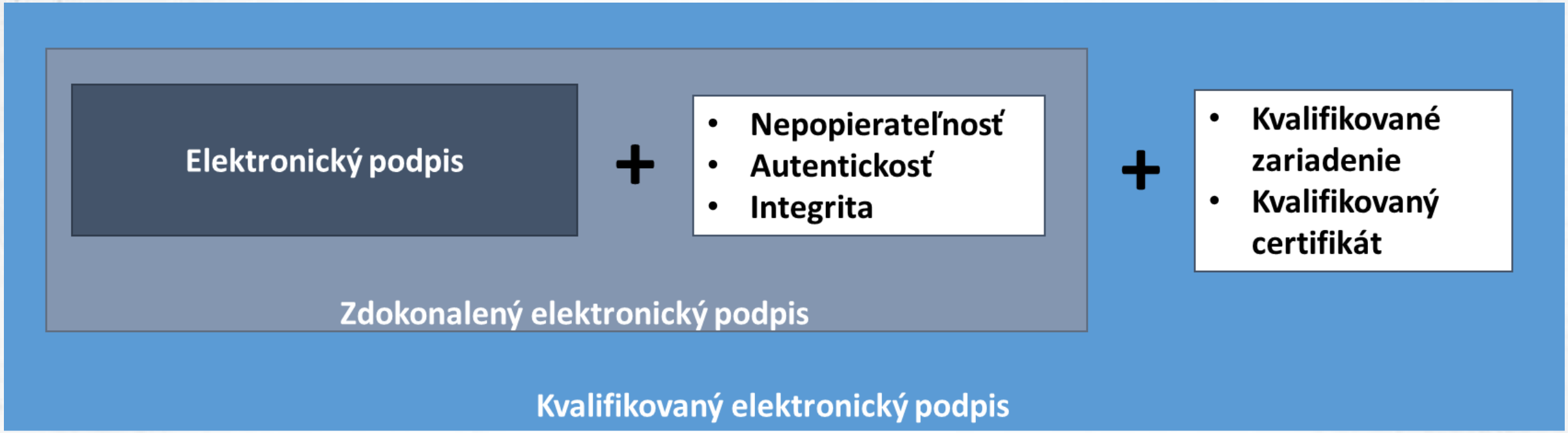


Elektronický podpis (I.)

- Právna úprava
  - NARIADENIE EURÓPSKEHO PARLAMENTU A RADY (EÚ) č. 910/2014 o elektronickej identifikácii a dôveryhodných službách pre elektronické transakcie na vnútornom trhu (**Nariadenie eIDAS**) a o zrušení smernice 1999/93/ES
  - Zákon č. 272/2016 Z. z. o dôveryhodných službách
- 3 typy elektronického podpisu:
  - **(obyčajný) elektronický podpis**
  - **zdokonalený elektronický podpis**
  - **kvalifikovaný elektronický podpis**

- vyšší typ elektronického podpisu -> lepšie technické zabezpečenie -> väčšia právna istota
- rôzna forma technickej realizácie - email, naskenovaný podpis, dynamické biometrické podpisy ...

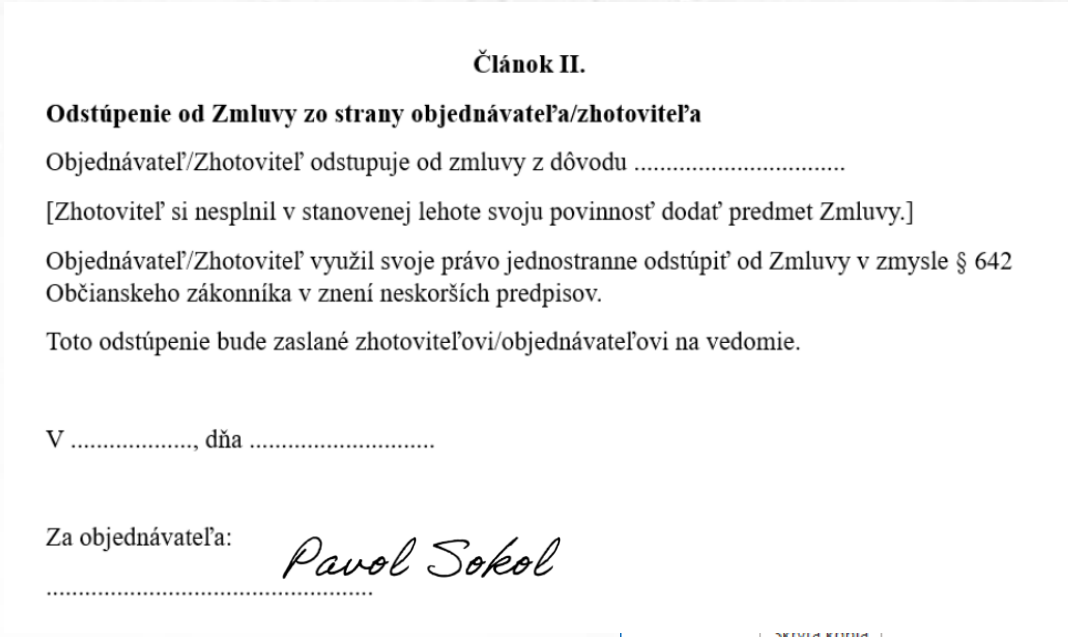
Elektronický podpis (II.)



(Obyčajný) elektronický podpis (I.)

(Obyčajný) elektronický podpis

- sú údaje v elektronickej forme, ktoré sú pripojené alebo logicky pridružené k iným údajom v elektronickej forme a ktoré podpisovateľ používa na podpisovanie;
- zákon o elektronickom podpise - nepoznal tento typ v takomto znení
- technická realizácia – podpis v rámci elektronickej pošty, naskenovaný podpis, dynamické biometrické podpisy ...



Článok II.

Odstúpenie od Zmluvy zo strany objednávateľa/zhotoviteľa

Objednávateľ/Zhotoviteľ odstupuje od zmluvy z dôvodu .....

[Zhotoviteľ si nesplnil v stanovenej lehote svoju povinnosť dodať predmet Zmluvy.]

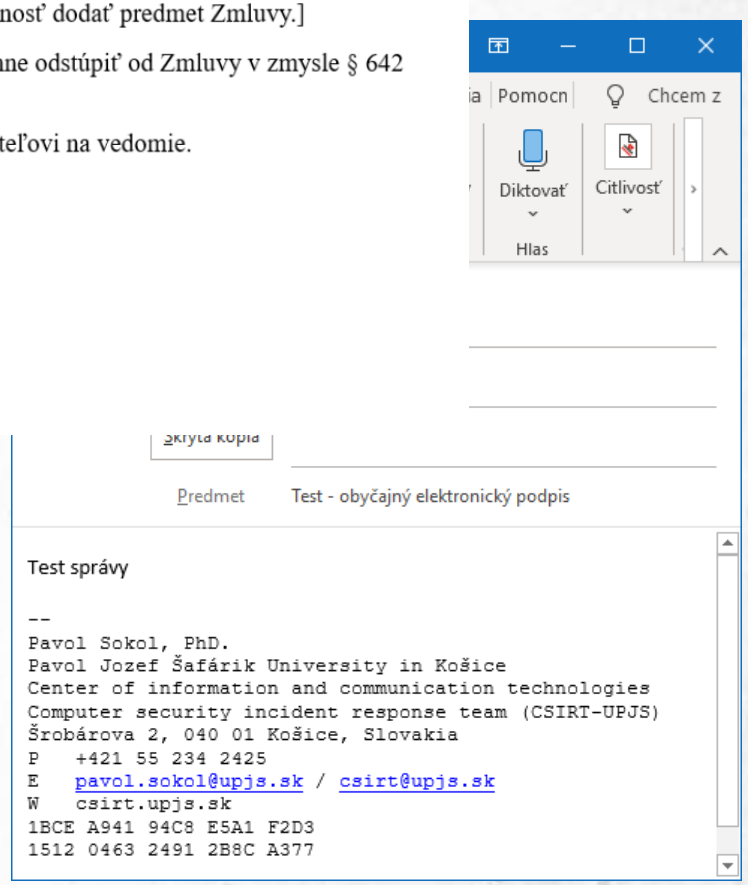
Objednávateľ/Zhotoviteľ využil svoje právo jednostranne odstúpiť od Zmluvy v zmysle § 642 Občianskeho zákonníka v znení neskorších predpisov.

Toto odstúpenie bude zaslané zhotoviteľovi/objednávateľovi na vedomie.

V ....., dňa .....

Za objednávateľa: Pavol Sokol

.....



Zdokonalený elektronický podpis (I.)

- je elektronický podpis, ktorý musí spĺňať ďalšie požiadavky.
- zákon o EP - elektronický podpis

- **Zdokonalený elektronický podpis**
  a) je **jedinečne spojený s podpisovateľom (nepopierateľnosť podpisovateľa)**
  b) umožňuje **určenie totožnosti** podpisovateľa **(autentifikácia podpisovateľa)**
  c) je **vyhotovený pomocou údajov** na vyhotovenie elektronického podpisu, ktoré môže podpisovateľ s vysokou mierou dôveryhodnosti používať pod **svojou výlučnou kontrolou (nepopierateľnosť podpisovateľa)**
  d) je prepojený s údajmi, ktoré sa ním podpisujú, takým spôsobom, že každú **dodatočnú zmenu údajov možno zistiť (integrita podpisovaného elektronického dokumentu)**

Zdokonalený elektronický podpis (II.)

- technická realizácia – princíp technologickej neutrality
- Požiadavky na technickú realizáciu:
  - **Autentickosť (Authenticity)** – rozpoznanie a jednoznačná identifikácia osoby podpisujúcej určitý dokument v konkrétnom čase,
  - **Integrita (Integrity)** – zaručenie nezmenenia údajov počas doby od podpísania po overenie podpisu,
  - **Nepopierateľnosť (Nonrepudiation)** – znemožnenie podpisovateľovi poprieť, že dokument podpísal on
- existujúca technická realizácia – **digitálny podpis**
  - asymetrická kryptografia – súkromný a verejný kľúč

Kvalifikovaný elektronický podpis (I.)

- **Kvalifikovaný elektronický** podpis je zdokonalený elektronický podpis, ktorý navyše je:
  - vyhotovený s použitím **kvalifikovaného zariadenia** na vyhotovenie elektronického podpisu
  - založený na **kvalifikovanom certifikáte** pre elektronické podpisy
  - technická realizácia – súkromný a verejný kľúč

Zdroj: https://www.slovensko.sk/sk/faq/faq-eid/

Kvalifikovaný elektronický podpis (II.)

- **Právny účinok elektronického podpisu** a jeho prípustnosť ako dôkazu v súdnom konaní sa nesmie odmietnuť výlučne z toho dôvodu, že **má elektronickú formu** alebo že nespĺňa požiadavky pre kvalifikované elektronické podpisy.

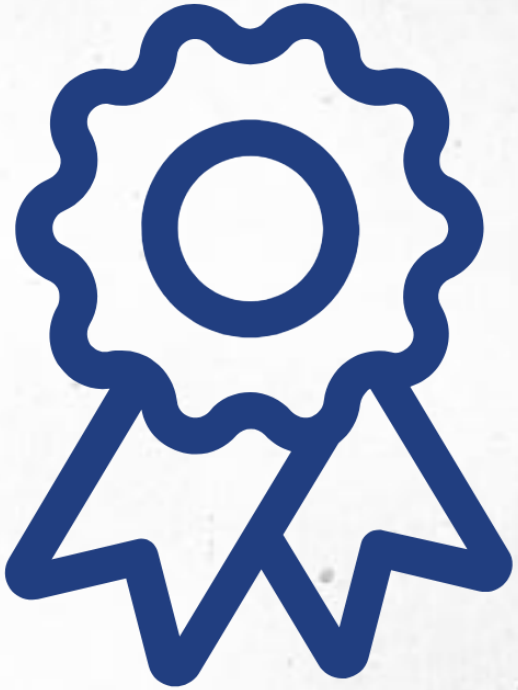
- **Kvalifikovaný elektronický podpis** má právny účinok rovnocenný s **vlastnoručným podpisom.**

- **Kvalifikovaný elektronický podpis založený na kvalifikovanom certifikáte** vydanom v jednom členskom štáte sa uznáva ako kvalifikovaný elektronický podpis vo všetkých **ostatných členských štátoch. -> zabezpečenie interoperability**

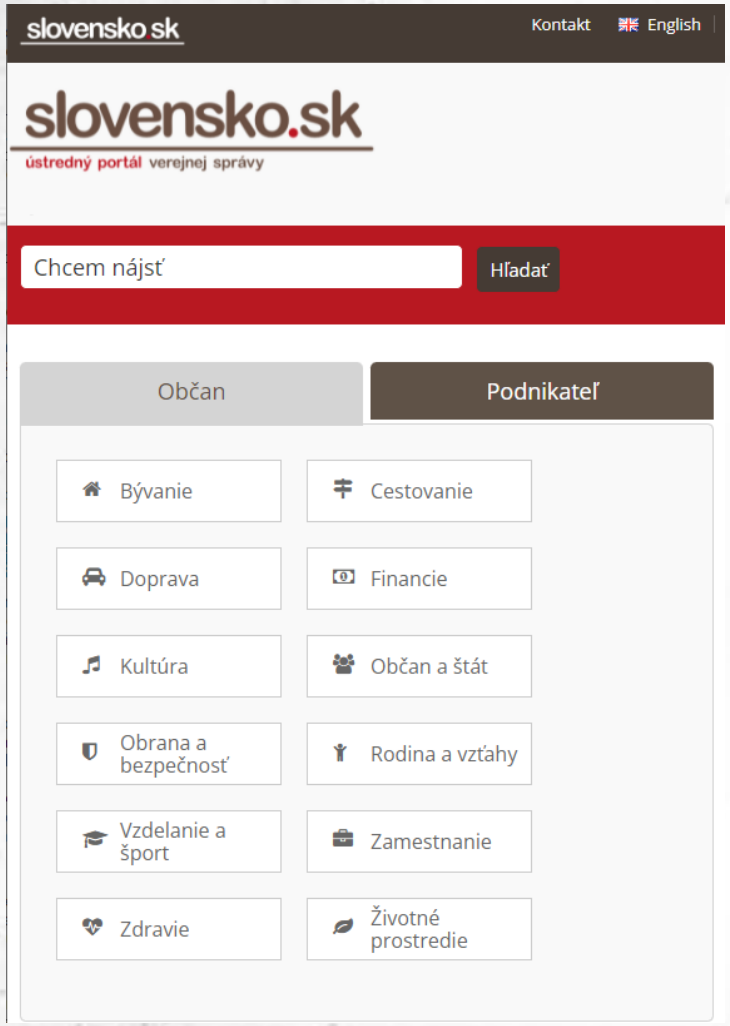
Služby vytvárajúce dôveru (I.)

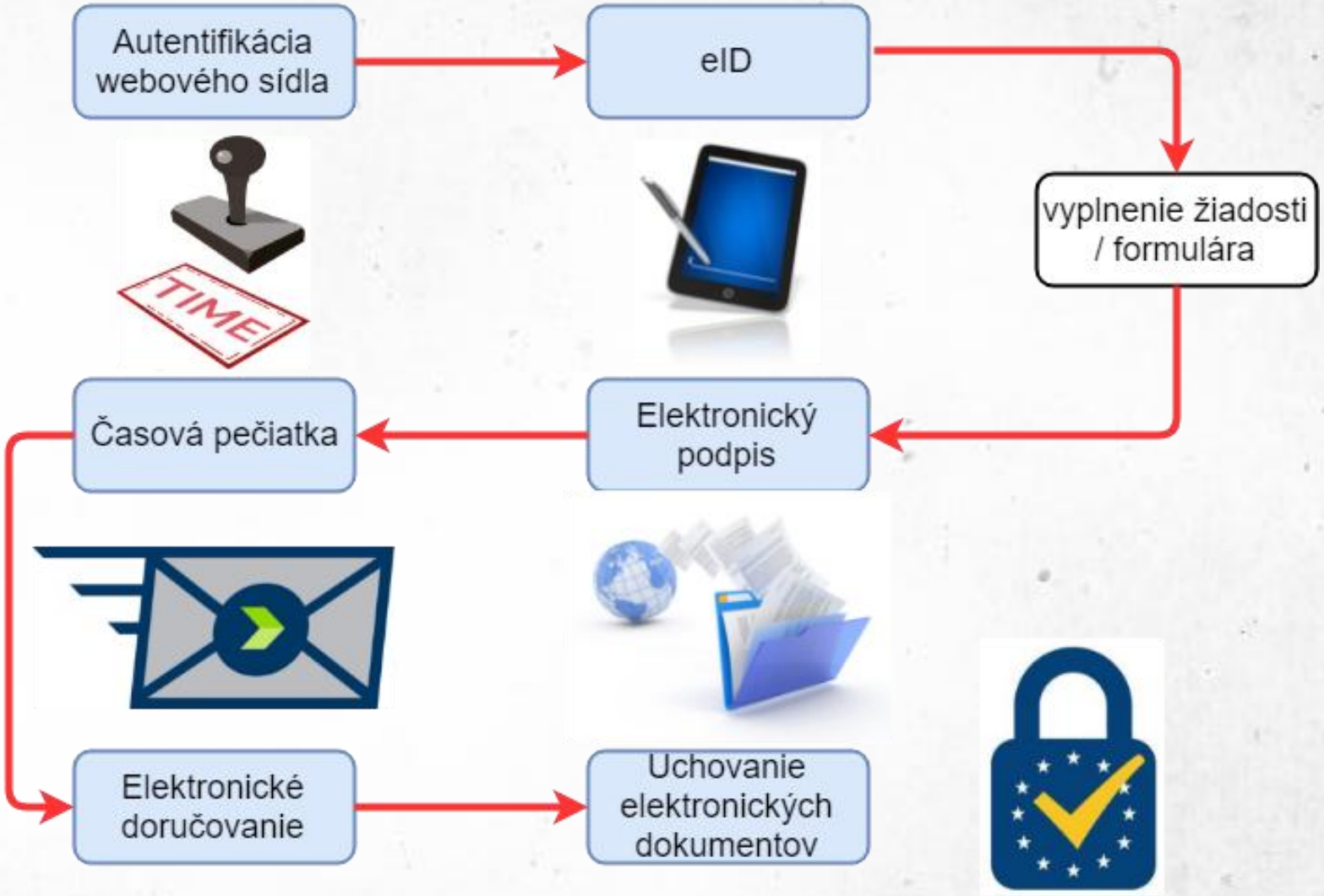
- Dôvera (Trust)

- Elektronická identifikácia
- Služby vytvárajúce dôveru
  - Elektronické podpisy
  - Elektronické pečate
  - Elektronické časové pečiatky
  - Elektronické doručovacie služby pre registrované zásielky
  - Autentifikácia webových sídiel
- Elektronické dokumenty
- Elektronické doručovanie



Služby vytvárajúce dôveru (II.)





Zdroj: https://www.slovensko.sk/sk/titulna-stranka

Smartfóny sú všade

6.64Billion

smartphone users in the world today

83.72%

of people have smartphones today

Zdroj: https://www.bankmycell.com/blog/how-many-phones-are-in-the-world

Využitie

- Chat, hovory, videohovory
- Fotenie
- Internet banking
- Bezkontaktné platby
- Navigácia
- Kľúče od auta
- Doklady
- Druhý faktor pri overovaní
- Sledovanie aktivít
- ....

Mobilné telefóny ako terč útokov

Internet bankingy slovenských bánk ohrozuje nebezpečný malware, dokáže obísť aj dvojfaktorovú autorizáciu

Softvér Pegasus nasadili v Maďarsku na sledovanie vyše stovky osôb

Zdroj: https://www.nextech.sk/a/Internet-bankingy-slovenskych-bank-ohrozuje-nebezpecny-malware--dokaze-obist-aj-dvojfaktorovu-autorizaciu, https://www.sme.sk/svet/c/softver-pegasus-nasadili-v-madarsku-na-sledovanie-vyse-stovky-osob, https://touchit.sk/pegasus-dokaze-sledovat-telefony-aj-na-slovensku/646885/

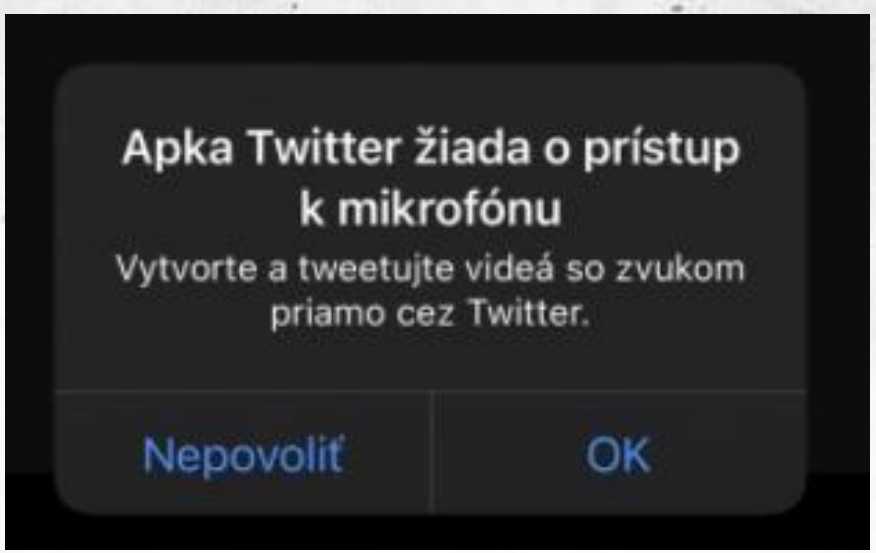
Ako také útoky prebiehajú?

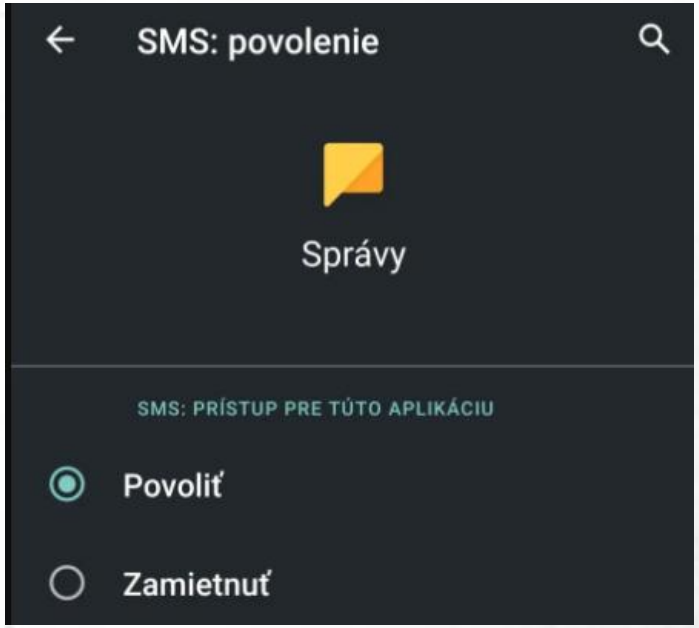
- Aplikácie štandardne bežia v tzv. sandboxe
- **Sandbox** je izolované prostredie, v ktorom bežia aplikácie s obmedzenými oprávneniami
- V sandboxe majú len veľmi limitované oprávnenia

Zdroj: https://www.goguardian.com/glossary/what-is-sandbox-security

Pieskovisko pre aplikácie

- Citlivé prístupy mimo pieskovisko vyžadujú schválenie užívateľa – tzv. **povolenie**
- Práve niektoré povolenia zneužívajú útočníci
- Cieľom je **zmanipulovať používateľa** k udeleniu požadovaných povolení





Zneužívané povolenia - SMS

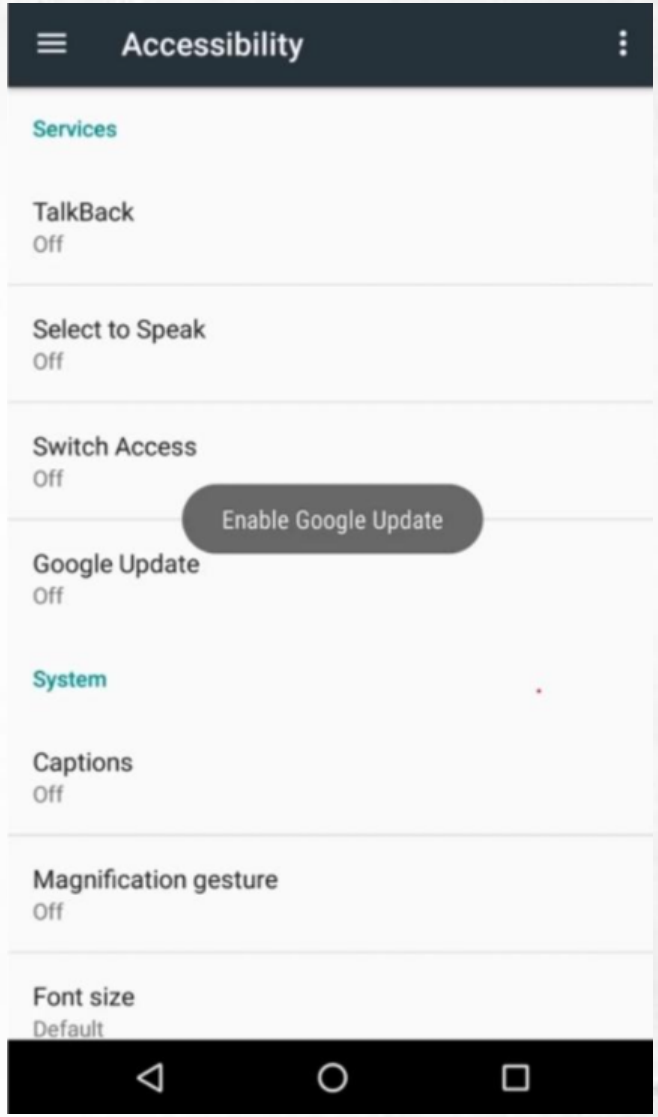
- Povolenie na SMS sa zneužíva na **odcudzenie overovacích kódov** (napríklad do internet bankingu)
- Útočníci tak vedia obísť aj účty chránené dvojfaktorovým overením

Služby na zjednodušenie ovládania

- Android podporuje inštaláciu „**služieb na zjednodušenie ovládania**“
- Tieto služby umožňujú **prekrývať** obrazovku, či zadávať text
- To má pomôcť používateľom so zrakovým či telesným postihnutím používať telefón

Služby na zjednodušenie ovládania (II.)

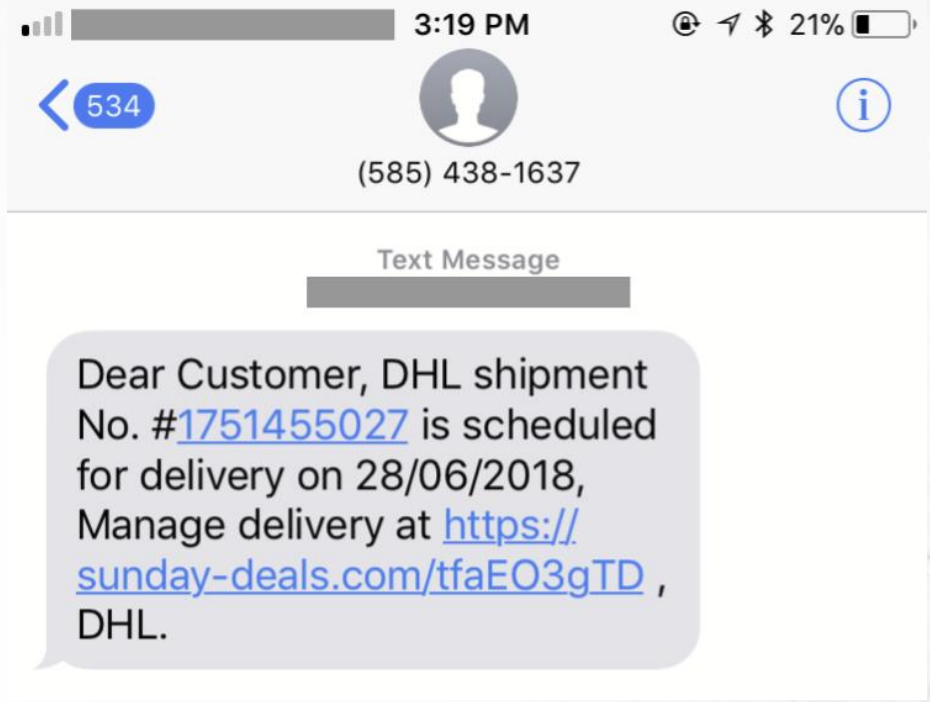
- Útočníci využívajú dané oprávnenia na **odcudzenie hesiel** a prihlasovacích údajov
- Okno aplikácie prekryjú svojim, neviditeľným, oknom, čo im umožňuje zachytávať všetky zadané dáta



Zdroj: https://gizmeek.com/everything-you-need-to-know-about-new-android-2020-virus-black-rock

Zneužívanie bezpečnostných zraniteľností

- Nie každý škodlivý softvér však vyžaduje schválenie používateľom
- Niekedy stačí **otvorenie škodlivej webovej** stránky či iba prijatie textovej správy
- Útočníci na to potrebujú **zneužiť bezpečnostné zraniteľnosti** v kóde



Zdroj: https://www.kaspersky.com/blog/how-to-protect-from-pegasus-spyware/43453/

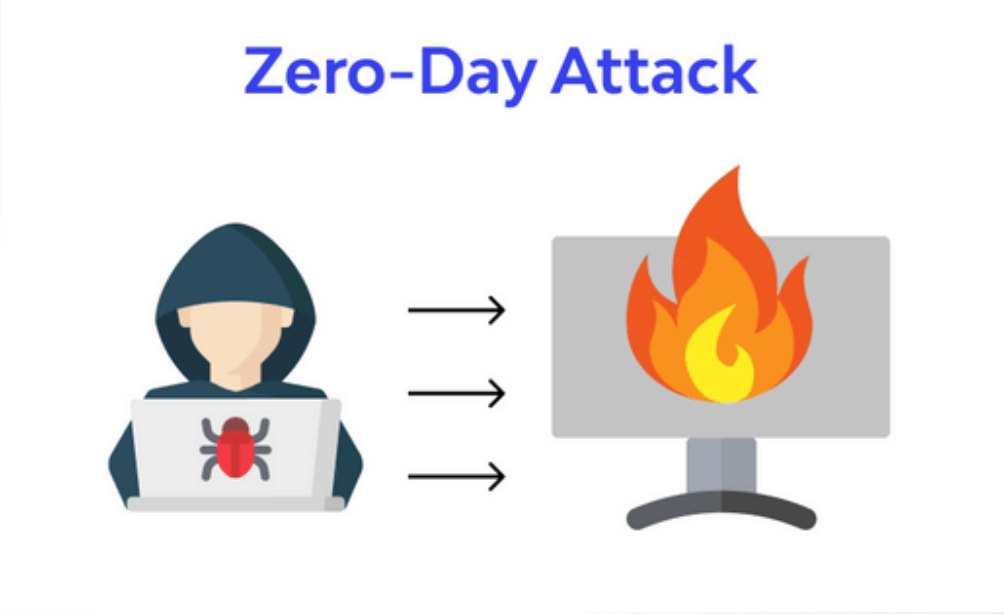
Zneužívanie bezpečnostných zraniteľností (II.)

- Rozlišujeme dva typy zraniteľností:
  - Zero-day
  - N-day
- **Zero-day** sú pre verejnosť neznáme, neopravené zraniteľnosti
- **N-day** sú už opravené zraniteľnosti

Zdroj: https://www.wallarm.com/what/explanation-of-the-zero-day-attack

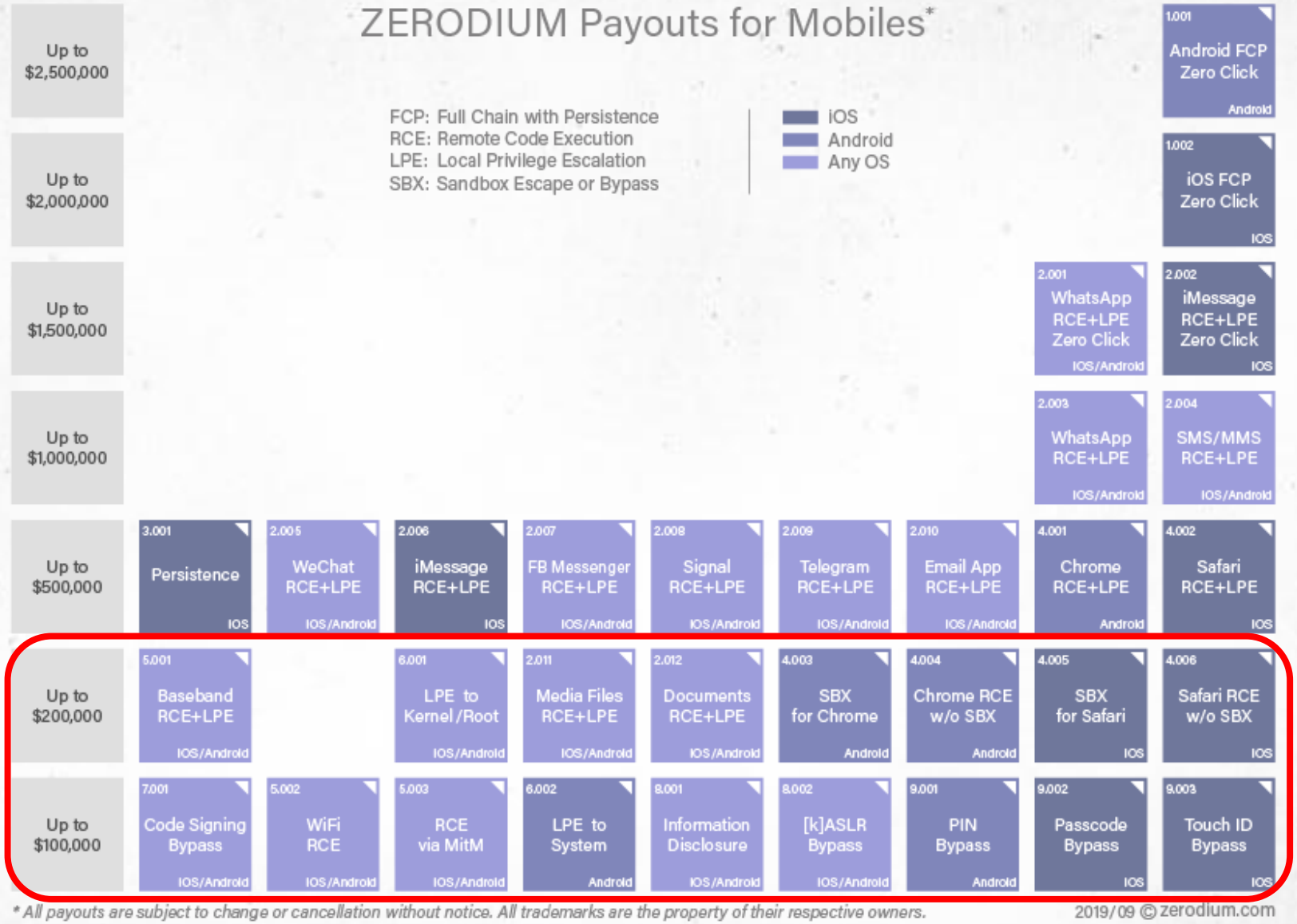
Zneužívanie bezpečnostných zraniteľností (III.)

- **Zero-day** zraniteľnosti sú zneužívané aj armádami a tajnými službami
- **N-day** zraniteľnosti využíva aj „bežný“ škodlivý softvér
- Proces zneužívania zraniteľnosti sa nazýva **exploitácia**



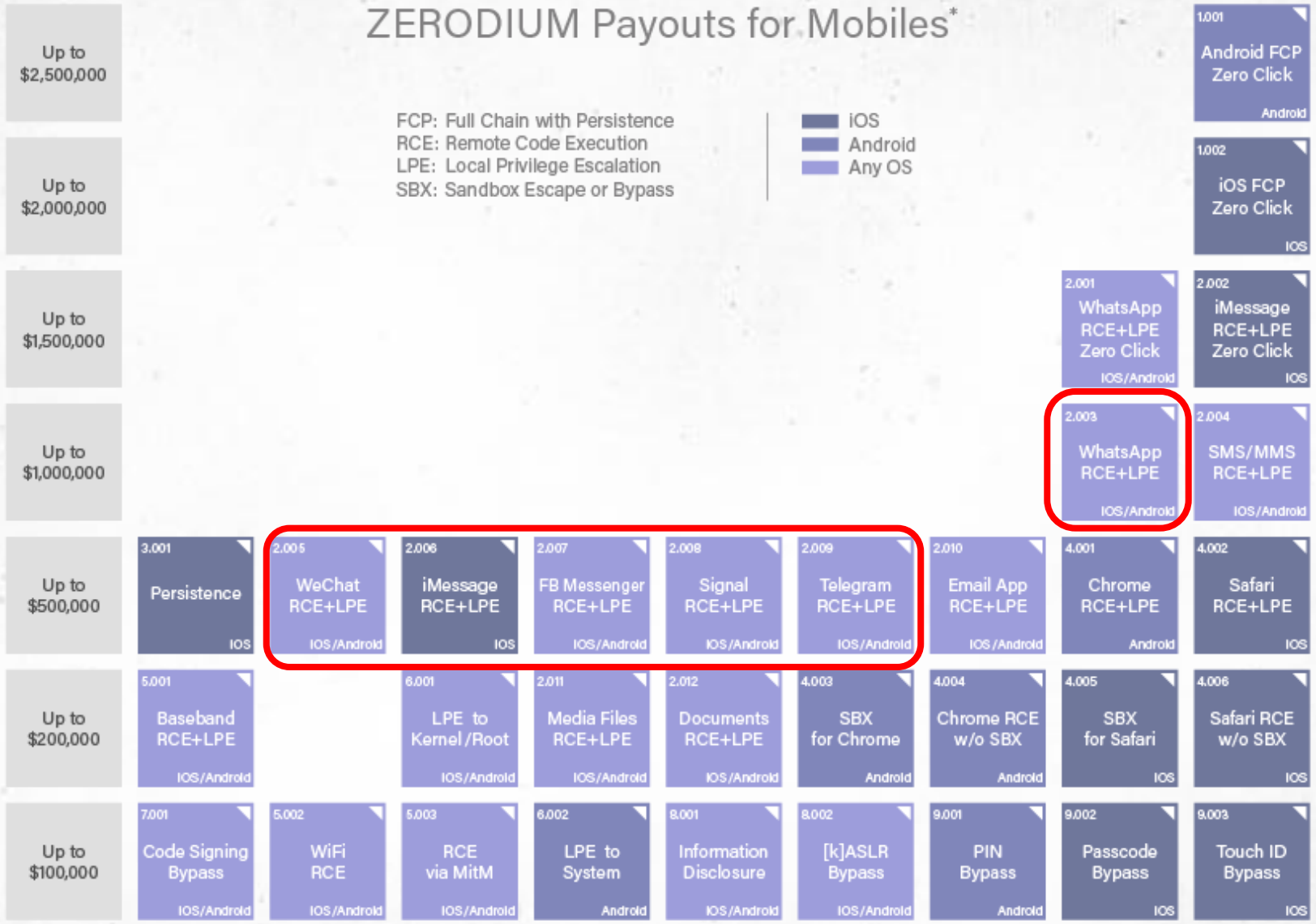
Zdroj: https://www.kaspersky.com/blog/how-to-protect-from-pegasus-spyware/43453/

Hodnota zraniteľností (I.)



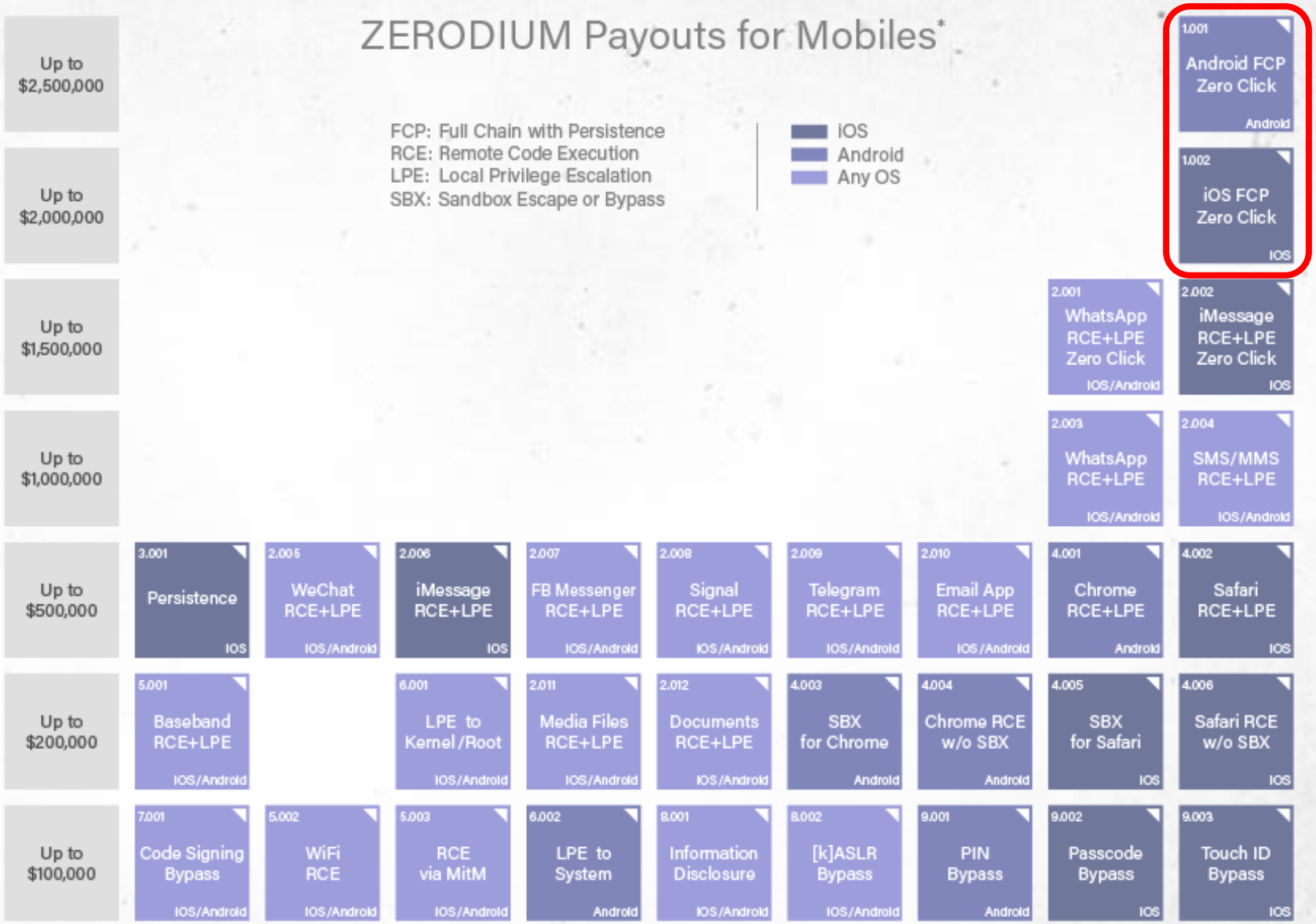
Zdroj: https://lab.wallarm.com/zero-day-marketplace-explained-how-zerodium-bugtraq-and-fear-contributed-to-the-rise-of-the-zero-day-vulnerability-black-market/

Hodnota zraniteľností (II.)



Zdroj: https://lab.wallarm.com/zero-day-marketplace-explained-how-zerodium-bugtraq-and-fear-contributed-to-the-rise-of-the-zero-day-vulnerability-black-market/

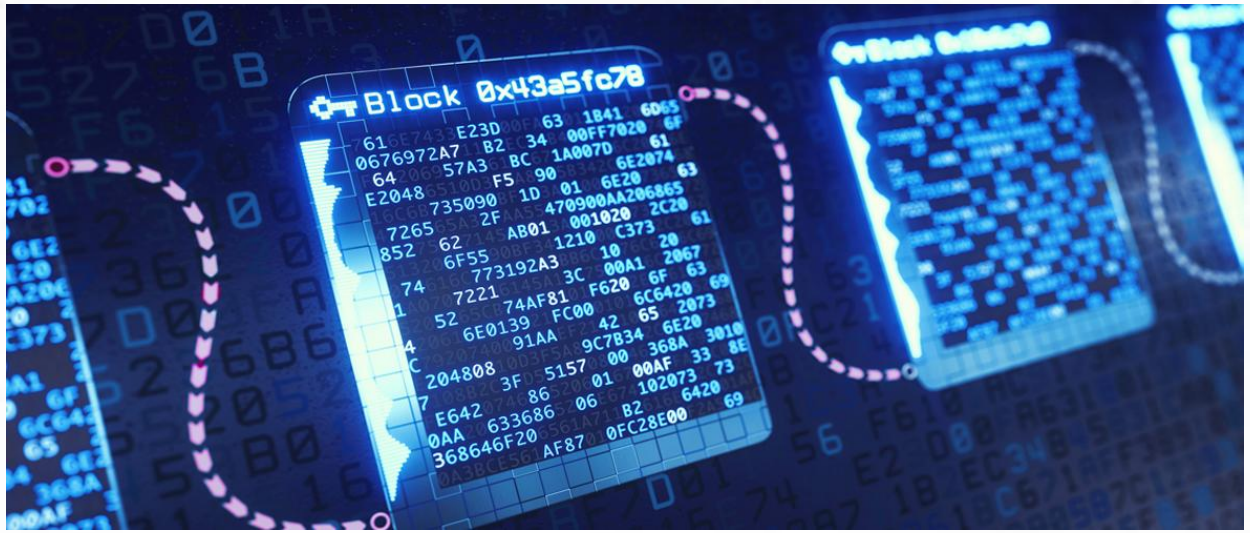
Hodnota zraniteľností (III.)



Zdroj: https://lab.wallarm.com/zero-day-marketplace-explained-how-zerodium-bugtraq-and-fear-contributed-to-the-rise-of-the-zero-day-vulnerability-black-market/

Exploitácia mobilných telefónov (I.)

- Vďaka množstvu bezpečnostných mechanizmov je exploitácia telefónov nesmierne zložitá
- Častokrát je nutné **zneužiť niekoľko zraniteľností súčasne**



Zdroj: https://www.tenable.com/blog/a-look-at-the-vulnerability-to-exploit-supply-chain

Exploitácia mobilných telefónov (II.)

- Štandardne „reťaz“ zraniteľností vyzerá nasledovne:
  1. Zneužitie zraniteľnosti na **spustenie kódu** vo webovom prehliadači
  2. Zneužitie zraniteľnosti na **uniknutie zo „sandboxu“** prehliadača
  3. Niekedy sa využívajú aj ďalšie zraniteľnosti, napríklad na obídenie anti-exploitačných mechanizmov, či pretrvanie v telefóne aj po reštarte (perzistencia)

Ako si vybrať bezpečný telefón? (I.)

- Najdôležitejšie sú **aktualizácie**
- Ako dlho ich bude telefón dostávať?
- Dva hlavné parametre:
  - Počet veľkých aktualizácií
  - Doba vydávania bezpečnostných záplat

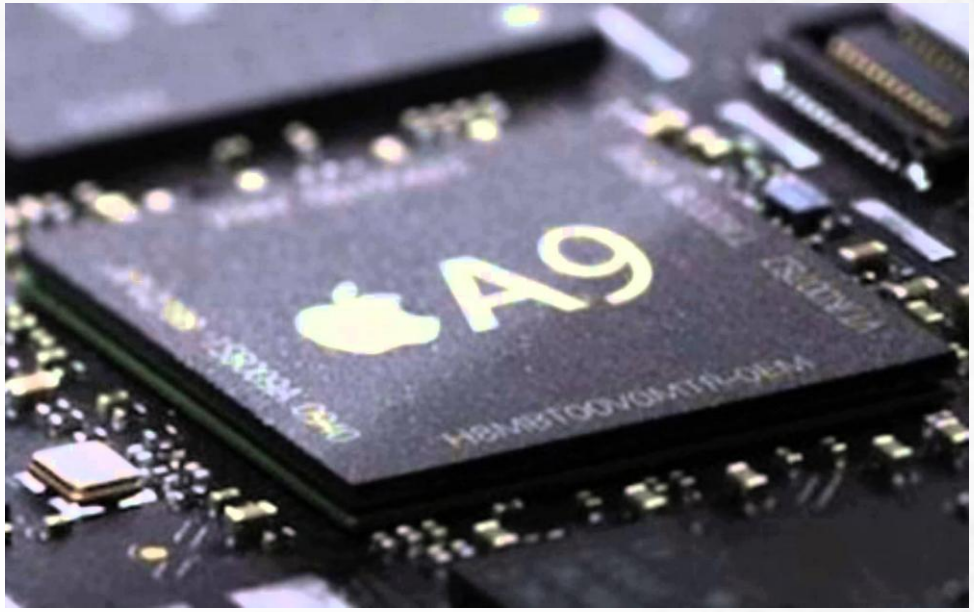
Ako si vybrať bezpečný telefón? (II.)

- Sú aj iné parametre, aj keď nie sú tak dôležité ako aktualizácie
- **Biometrické overenie**
  - Optické skenery odtlačkov prstov sú menej bezpečné než kapacitné a ultrasonické

Zdroj: https://www.theverge.com/circuitbreaker/2018/3/12/17109114/samsung-galaxy-note-9-no-in-display-fingerprint-sensor-ming-chi-kuo-kgi-rumor

Ako si vybrať bezpečný telefón? (III.)

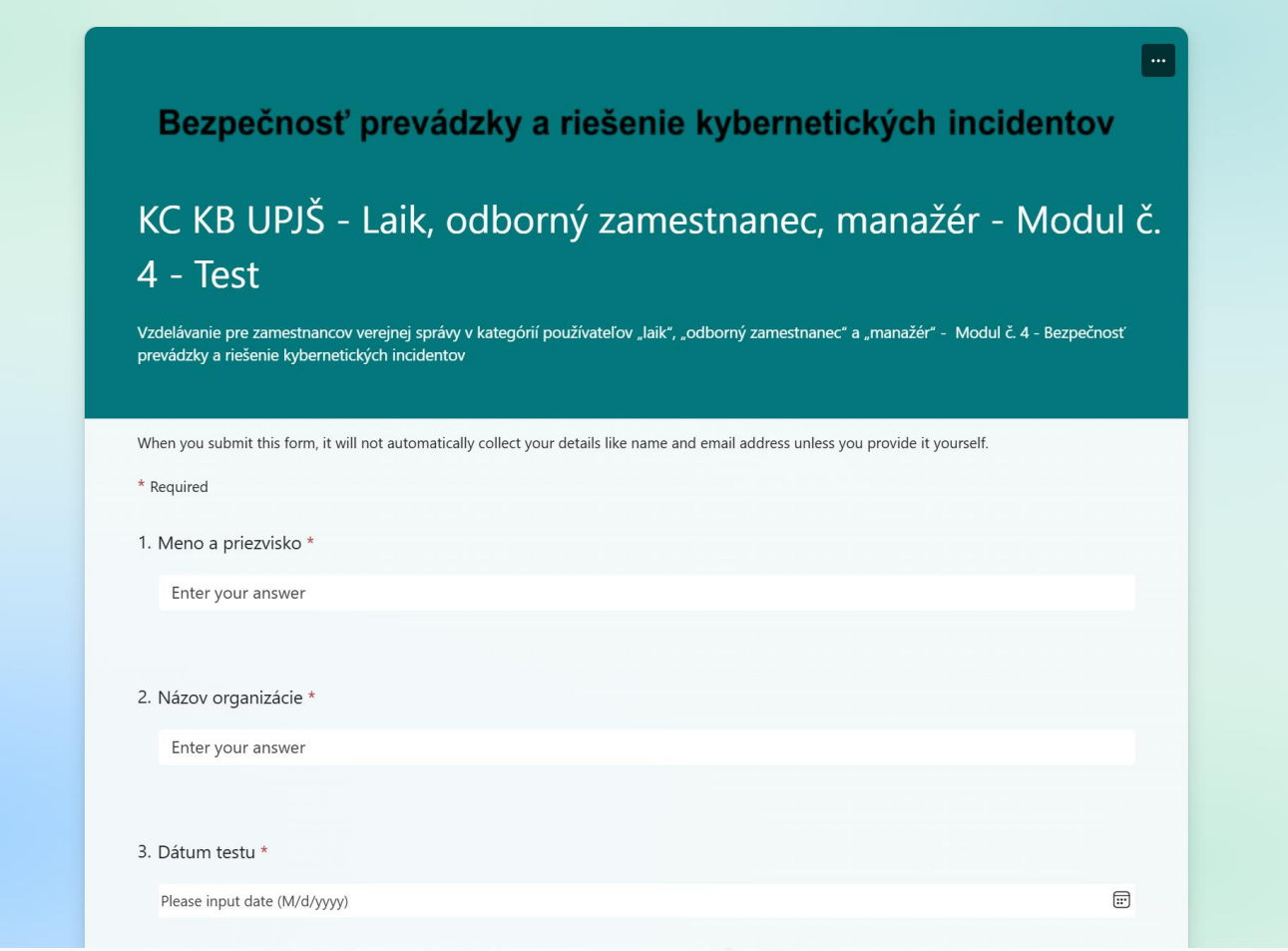
- **Procesor** má výrazný vplyv na bezpečnosť
- **MediaTek** procesory sú považované za menej bezpečné než konkurencia
- Pri Apple zariadeniach sú zariadenia s **Apple A12=<** výrazne bezpečnejšie než zariadenia so staršími procesormi



Zdroj: https://ios.gadgethacks.com/how-to/check-if-your-iphone-6s-6s-plus-is-victim-chipgate-0165306/

Záverečný test / Diskusia

- Test: ...



Bezpečnosť prevádzky a riešenie kybernetických incidentov

KC KB UPJŠ - Laik, odborný zamestnanec, manažér - Modul č. 4 - Test

Vzdelávanie pre zamestnancov verejnej správy v kategórií používateľov „laik“, „odborný zamestnanec“ a „manažér“ - Modul č. 4 - Bezpečnosť prevádzky a riešenie kybernetických incidentov

When you submit this form, it will not automatically collect your details like name and email address unless you provide it yourself.

* Required

1. Meno a priezvisko *

Enter your answer

2. Názov organizácie *

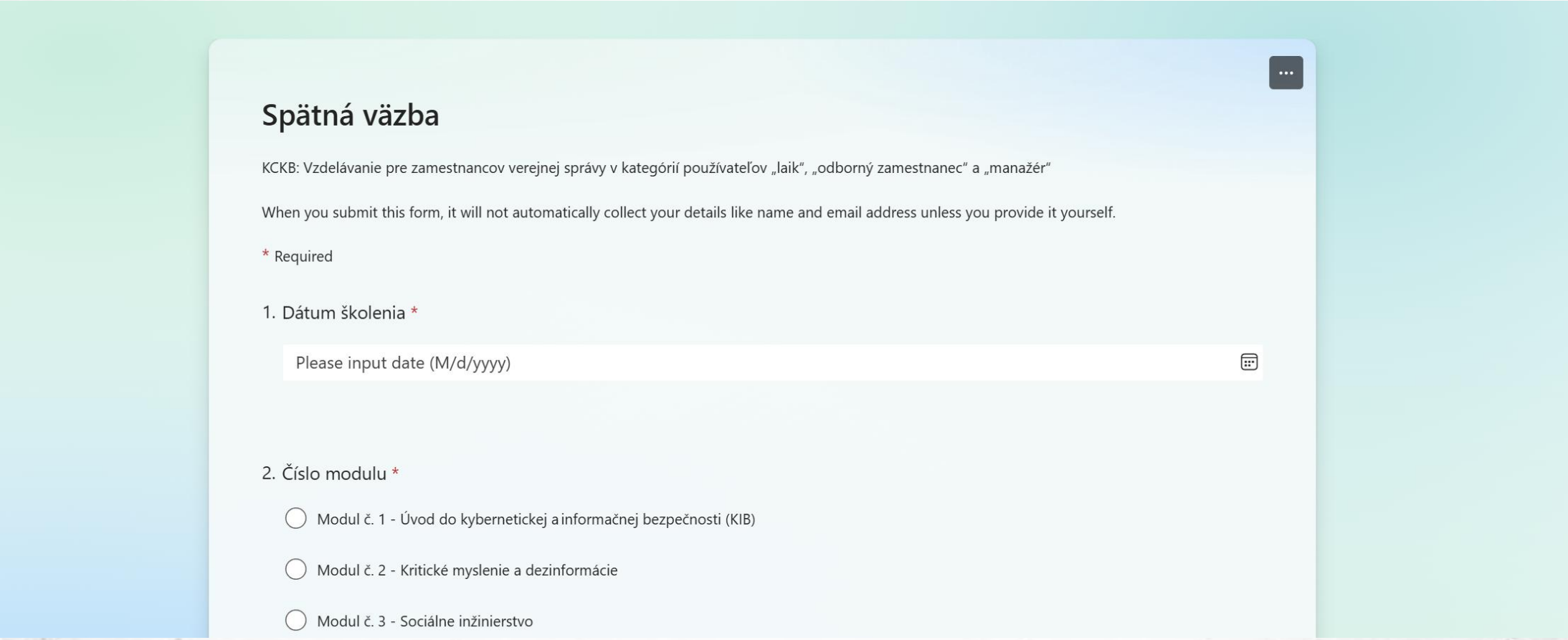
Enter your answer

3. Dátum testu *

Please input date (M/d/yyyy)

Spätná väzba

- Spätná väzba: ...



Spätná väzba

KCKB: Vzdelávanie pre zamestnancov verejnej správy v kategórií používateľov „laik“, „odborný zamestnanec“ a „manažér“

When you submit this form, it will not automatically collect your details like name and email address unless you provide it yourself.

* Required

1. Dátum školenia *

Please input date (M/d/yyyy)

2. Číslo modulu *

- Modul č. 1 - Úvod do kybernetickej a informačnej bezpečnosti (KIB)
- Modul č. 2 - Kritické myslenie a dezinformácie
- Modul č. 3 - Sociálne inžinierstvo

KCKB UPJS

UNIVERZITA PAVLA JOZEFA ŠAFÁRIKA V KOŠICIACH

Financované Európskou úniou NextGenerationEU

PLÁN OBNOVY

MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY

Ďakujem za pozornosť

meno.priezvisko@upjs.sk

https://cyberawareness.sk